普通高等学校本科专业设置申请表

校长签字：

学校名称（盖章）：沈阳化工大学

学校主管部门：辽宁省

专业名称：网络空间安全

专业代码：080911TK

所属学科门类及专业类：工学 计算机类

学位授予门类：工学

修业年限：四年

申请时间：2025-07-23

专业负责人：王军

联系电话：15940530506

教育部制

1.学校基本情况

学校名称	沈阳化工大学	学校代码	10149
主管部门	辽宁省	学校网址	http://www.syuct.edu.cn/
学校所在省市区	辽宁沈阳辽宁省沈阳市经济技术开发区11号街	邮政编码	110142
学校办学基本类型	☐教育部直属院校 ☐其他部委所属院校 ☑地方院校		
	☑公办 ☐民办 ☐中外合作办学机构		
已有专业学科门类	☐哲学 ☑经济学 ☑法学 ☑教育学 ☑文学 ☐历史学 ☑理学 ☑工学 ☐农学 ☐医学 ☑管理学 ☑艺术学		
学校性质	☐综合 ☑理工 ☐农业 ☐林业 ☐医药 ☐师范 ☐语言 ☐财经 ☐政法 ☐体育 ☐艺术 ☐民族		
曾用名	沈阳化工学院、辽宁科学技术大学		
建校时间	1952	首次举办本科教育年份	1958年
通过教育部本科教学评估类型	审核评估	通过时间	2025年05月
专任教师总数	1028	专任教师中副教授及以上职称教师数	396
现有本科专业数	47	上一年度全校本科招生人数	4325
上一年度全校本科毕业人数	3461		
学校简要历史沿革	沈阳化工大学始建于1952年，1958年升格为本科，名为沈阳化工学院，1960年更名辽宁科学技术大学，1962年更名沈阳化工学院隶属化学工业部，1998年变为“中央与地方共建，以地方管理为主”，2010年更名沈阳化工大学，是省“双一流”重点建设高校，国家“中西部高校基础能力建设工程”重点建设高校等。		
学校近五年专业增设、停招、撤并情况	学校近五年新增专业4个应急管理、大数据管理与应用、人工智能、新能源材料与器件。 撤销专业共13个，材料物理、资源环境科学、环境科学、工业工程、理论与应用力学、服装与服饰设计、工业设计、电子信息科学与技术、信息与计算科学、市场营销、信息管理与信息系统、公共事业管理、通信工程。 停招专业共12个，机械电子工程、视觉传达设计包装工程、复合材料与工程、林产化工、资源循环科学与工程、水质科学与技术、食品科学与工程、工		

	商管理、大数据管理与应用、应用物理学、物联网工程。

2.申报专业基本情况

申报类型	新增国控专业		
专业代码	080911TK	专业名称	网络空间安全
学位授予门类	工学	修业年限	四年
专业类	计算机类	专业类代码	0809
门类	工学	门类代码	08
申报专业类型	新建专业	原始专业名称	-
所在院系名称	计算机科学与技术学院		
学校现有相近专业情况			
相近专业1专业名称	计算机科学与技术（注：可授理学或工学学士学位）	开设年份	1989年
相近专业2专业名称	网络工程	开设年份	2009年
相近专业3专业名称	-	开设年份	-

3.申报专业人才需求情况

申报专业主要就业领域	网络空间安全专业的毕业生可在各类网络生产使用单位进行设备安全检测、方案设计、系统集成、咨询、技术支持维护、网络安全评估、网络安全保障等岗位工作。可从事的工作领域如下： 1.政府各级单位的网络信息安全保障。按照信息安全等级保护相关要求，开展基于密级标识的涉密信息及载体管控。 2.电信和网络运营企业，需要各级别的网络信息安全人才维护网络安全环境、监测网络安全风险、排除网络安全隐患，维护民用网络正常运行。 3.网警网监单位，需要专业级别的网络信息安全人才进行网络保密检查、失泄密核查取证、网络犯罪的核查取证等。 4.金融信息安全领域，需要大量的专业级别的网络信息安全人才、数据安全人才对有线和无线金融网络支付业务系统提供安全运维、安全防护及安全开发、数据治理。 5.能源行业在电力电网、石油石化需要大量的专业级别的网络信息安全人才进行能源运输系统的网络的保障。

	6.工业控制系统和轨道交通领域，按照信息安全等级保护相关要求，建设完善安全可控的控制系统，需要大量的专业网络信息安全人才建立以杜绝重大灾难性事件为底线的控制系统综合安全防护体系，建立完善控制信息安全技术与管理。	
人才需求情况	我校专业建设工作组对辽宁省及周边省市用人单位、合作企业的调研后，总结出网络空间安全专业的人才需求呈现以下特点：1）网络安全研发及服务企业、网络集成服务商的年需求人数多；2）企事业单位、智能制造企业年需求少，但用人单位数量多；3）网络安全人才普通本科的网络安全从业者占比较高，安全服务与运维类岗位需求量最多，应用型本科院校培养人才具有更大的就业面。以下是部分企业的人才需求情况： 1.杭州安恒信息技术股份有限公司，年均100人，主要需求岗位覆盖销售工程师、安全服务工程师（漏洞方向）、安全研究员、解决方案工程师、安全产品开发工程师、安全运维工程师等岗位。其中安恒信息下属辽宁分公司，年均20人，主要需求集中于安全服务工程师、安全运维工程师。 2.奇安信科技集团股份有限公司，年均50人，主要需求岗位覆盖安全监测分析工程师、安全研究工程师、渗透测试工程师、安全产品开发工程师等岗位。 3.北方实验室（沈阳）股份有限公司，年均10人，安全售前工程师、安全集成工程师、前端开发工程师、渗透测试工程师等岗位。 4.南京迈特望科技股份有限公司，年均20人，安全销售经理、安全售前工程师、安全运维工程师、安全解决方案工程师等岗位。 5.京北方信息技术股份有限公司，年均25人，安全售前工程师、安全集成工程师等岗位。 6.爱多邦（北京）信息技术服务有限公司，年均20人，安全驻场服务工程师、安全产品售后工程师、安全产品解决方案工程师等岗位。 7.沈阳星翼信息科技有限公司，年均10人，安全培训工程师，安全服务工程师等岗位。 8.东软集团有限公司，年均20人，数据安全工程师、漏洞挖掘工程师、应急响应工程师。 9.辽宁三色系统集成服务有限公司，年均20人 ，AI安全的算法/网络安全/大数据类等岗位。 10.中国移动通信集团有限公司辽宁分公司，年均20人，网络安全运营工程师，网络安全产品工程师、网络安全集成工程师等。	
申报专业人才需求调研情况	年度招生人数	30
	预计升学人数	6

	预计就业人数	24
	安恒信息辽宁分公司	6
	北方实验室（沈阳）股份有限公司	3
	奇安信科技集团股份有限公司	3
	京北方信息技术股份有限公司	2
	沈阳星翼信息科技有限公司	3
	东软集团有限公司	5
	辽宁三色系统集成服务有限公司	2

4. 产业调研报告

沈阳化工大学新增网络空间安全专业
面向行业产业人才需求调研报告

一、引言

1.1 调研背景与意义

在数字化时代，网络已深度融入社会经济的各个层面，网络空间安全的重要性日益凸显。据中国互联网络信息中心（CNNIC）发布的第 55 次《中国互联网络发展状况统计报告》显示，截至 2024 年 12 月，我国网民规模达 10.81 亿，互联网普及率达 76.4%。然而近年来，网络安全事件频繁爆发，各类供应链攻击事件影响广泛，波及众多政府机构和企业，充分暴露了网络安全防护体系的脆弱性，也凸显了网络空间安全在保障各行业稳定运行中的关键地位。

网络安全事件的频发对各行业产生了巨大冲击。例如，在金融行业，网络攻击可能导致客户资金被盗、金融数据泄露，进而引发客户信任危机，扰乱金融秩序；能源行业的网络安全事故则可能影响国家能源供应的稳定性，甚至危及国家安全。培养高素质的网络空间安全专业人才，对于各行业产业的安全、稳健发展至关重要。

本次调研深入了解网络空间安全行业产业对人才的需求状况，通过分析当前人才供需存在的问题，为优化我校网络空间安全专业人才培养方案提供有力依据，使人才培养与行业需求紧密对接，为我校培养适应社会需求的网络空间安全人才奠定基础。

1.2 调研目标

本调研旨在洞察网络空间安全行业产业人才需求的现状与未来趋势。通过多维度的研究，对未来行业所需人才的数量、层次、结构，以及在知识、能力、素质等方面的新要求进行科学研判。这些研究将为我校制定网络空间安全专业人才培养方案、更新教学内容提供关键依据，确保培养出的人才能够满足行业不断变化的需求，为网络空间安全领域注入源源不断的活力。

二、网络空间安全行业产业现状

2.1 行业发展历程与现状概述

网络空间安全行业的发展历程可追溯到 20 世纪 60 年代，随着美国国防部高级研究计划局（ARPA）网络的诞生，网络安全的需求也应运而生。1971 年，第一个计算机病毒 Creeper 出现，随后杀毒软件等网络安全防护工具逐渐发展起来。在 20 世纪 90 年代，随着互联网的商业化普及，网络空间安全行业开始迅速发展，防火墙、入侵检测系统等产品相继问世。

当前，网络空间安全市场规模持续增长。根据 IDC 的数据，2024 年全球网络安全市场规模达到 2233.4 亿美元，预计到 2029 年将增长至 3840.6 亿美元，年复合增长率为 10.7%。从

产业结构来看，网络安全市场主要包括网络安全硬件、软件和服务三大板块。其中，网络安全服务市场增长迅速，2024 年其市场份额占比达到 40.5%，这主要得益于企业对网络安全整体解决方案的需求不断增加。在细分领域，云计算安全、大数据安全、物联网安全等新兴领域发展势头强劲，成为推动网络空间安全行业发展的新动力。

2.2 主要行业产业应用场景中的网络安全状况

2.2.1 金融行业

金融行业的网络架构具有复杂性和高关联性的特点，涵盖了核心业务系统、支付清算系统、客户信息管理系统等多个关键系统。随着金融数字化的加速发展，金融行业面临的网络攻击类型日益多样化。据麦肯锡研究所的数据，基于 AI 的身份欺诈已成为美国增长最快的金融犯罪类型，并且在全球范围内呈上升趋势。英国 GDG 的研究表明，英国有超过 860 万人使用虚假或他人的身份来获取商品、服务或信贷。在美国，财政部发布的报告指出，AI 的发展使网络犯罪分子更容易使用深度伪造来冒充金融机构的客户并访问账户。另据德勤的数据，91% 的网络攻击都是从网络钓鱼电子邮件开始的。

在支付安全方面，金融行业采用了多种安全防护措施，如支付令牌化技术、实时风险监测系统等。客户信息保护则通过加密技术、访问控制等手段来实现，确保客户的个人信息和交易数据不被泄露。在交易系统安全方面，金融机构加强了对交易流程的监控，采用了分布式账本技术等新兴技术来提高交易的安全性和透明度。尽管如此，金融行业仍面临着严峻的网络安全挑战，如 2024 年美国一个金融机构遭受了大规模的网络钓鱼攻击，导致大量客户信息泄露，造成了巨大的经济损失和声誉影响。

2.2.2 能源行业

能源行业（电力、石油、天然气等）的关键基础设施网络架构复杂，涉及大量的工业控制系统。这些系统具有实时性强、可靠性要求高的特点，但同时也存在安全防护薄弱的问题。外部攻击方面，能源行业面临着黑客攻击能源控制系统的风险，一旦成功入侵，可能导致能源供应中断，影响社会正常运转。内部安全风险则主要来自于内部人员的违规操作，如误操作、恶意篡改数据等。

为应对这些安全风险，能源行业在工业控制系统安全方面采取了一系列措施，如部署工业防火墙、入侵检测系统等安全设备，加强对工业控制系统的网络隔离。在数据传输安全方面，采用加密技术确保数据在传输过程中的保密性和完整性。例如，国家电网在其智能电网建设中，投入大量资金用于网络安全防护，通过建立安全监测平台，实时监控网络安全态势，有效提升了电网的安全防护能力。然而，能源行业的网络安全防护仍存在一些不足之处，如部分老旧设备的安全漏洞难以修复，安全防护技术与业务系统的融合度有待提高等。

2.2.3 互联网行业

互联网企业的业务特点决定了其对网络安全的高度依赖。以网站安全为例，互联网企业需要防范 DDoS 攻击、SQL 注入攻击、跨站脚本攻击等多种安全威胁。据 Akamai 的报告，金融服务行业在 DDoS 攻击事件中的占比高达 34%，位居各行业之首，而互联网行业也是 DDoS 攻击的重点目标之一。在用户数据保护方面，互联网企业掌握着大量用户的个人信息，一旦发生数据泄露事件，将对用户权益造成严重损害，同时也会影响企业的声誉。

云计算安全是互联网行业面临的另一个重要挑战。随着云计算技术的广泛应用，云服务提供商需要保障云平台的安全，防止云租户数据泄露、云服务器被入侵等安全事件的发生。互联网行业在应对这些安全威胁时，采用了多种技术手段，如 DDoS 攻击防范采用流量清洗技术，漏洞管理通过定期进行漏洞扫描和修复来实现，内容安全审核则利用人工智能技术对用户生成的内容进行审核。尽管如此，互联网行业仍频繁遭受网络安全攻击，如 2024 年 Facebook 平台发生了大规模的数据泄露事件，涉及数亿用户的个人信息，引发了社会的广泛关注。

2.2.4 政府部门

政府部门在电子政务、公共服务平台等方面的网络安全需求日益迫切。随着政务信息化的推进，政府部门面临着网络间谍活动、政务数据泄露等安全挑战。在网络间谍活动方面，一些境外势力试图通过网络手段窃取政府的敏感信息，威胁国家主权和安全。政务数据泄露则可能导致公民个人信息泄露、政府公信力受损等问题。

为加强网络安全防护，政府部门在网络安全政策法规制定方面发挥了重要作用，出台了一系列法律法规，如《网络安全法》《数据安全法》等，为网络安全管理提供了法律依据。在安全管理体系建设方面，政府部门建立了完善的安全管理制度，明确了各部门的安全职责，加强了对网络安全事件的应急响应能力。在安全技术应用方面，采用了先进的加密技术、访问控制技术等，保障政务系统的安全运行。例如，中央网信办通过建立网络安全监测平台，对全国范围内的政务网络进行实时监测，及时发现和处置安全隐患。然而，政府部门在网络安全防护方面仍面临一些挑战，如网络安全人才短缺、不同部门之间的安全协同机制有待完善等。

2.2.5 工业生产场景

工业生产场景的网络安全正面临愈发严峻的挑战。随着工业互联网的深度渗透，传统封闭的工业控制系统（ICS）逐渐与外部网络连通，攻击面大幅扩大。据美国工业控制系统网络应急响应小组（ICS-CERT）2024 年报告显示，全球工业领域网络攻击事件较 2020 年增长 187%，这些攻击呈现出专业化、定向化特征，黑客往往针对特定工业协议（如 Modbus、Profinet）和设备固件漏洞实施精准打击，部分攻击甚至具备潜伏数月的持久化能力。

当前工业网络安全防护体系仍存在明显短板。一方面，大量老旧工业设备缺乏基本的安全功能，有些企业仍在使用 20 年前的 PLC 设备，未设置密码保护且无法升级固件，成为网络攻击的“突破口”。另一方面，工业生产的连续性要求与安全防护存在矛盾，多数企业因担心影响生产效率，不愿部署深度检测设备或进行频繁安全更新。据 Ponemon Institute 调研，仅 38% 的工业企业建立了专门的 ICS 安全团队，62%的企业承认工业网络与 IT 网络边界防护存在漏

洞。此外，工业数据安全防护不足，生产工艺参数、设备运行数据等敏感信息在传输和存储过程中面临泄露风险，给企业核心竞争力带来威胁。

三、网络空间安全专业人才现状

3.1 人才供给情况

3.1.1 高校培养情况

近年来，开设网络空间安全专业的高校数量不断增加。根据教育部公布的数据，截至2024年，全国已有超过200所高校开设了网络空间安全专业，招生规模逐年扩大，2024年该专业的本科招生人数达到了2万余人。从毕业生数量来看，随着首批网络空间安全专业学生的毕业，该专业的毕业生数量呈现出快速增长的趋势，2024年毕业生人数达到了1.5万余人。

然而，辽宁省内只有辽宁大学、沈阳工程学院、辽宁警察学院、大连东软信息学院四所高校设置网络空间安全专业，但年均培养量不足400人，远低于工业互联网、政务数字化等领域激增的需求，不足以支撑区域经济发展需求。

3.1.2 社会培训情况

社会上的网络空间安全培训机构类型多样，包括专业的网络安全培训机构、IT培训机构的网络安全课程等。这些培训机构的培训课程内容丰富，涵盖了网络安全的各个领域，如网络安全认证培训（如CISSP、CISA等）、网络攻防实战培训等。培训规模也在不断扩大，据不完全统计，2024年全国网络空间安全培训机构的培训学员数量超过了10万人次。

社会培训在人才培养方面具有灵活性和针对性的优势，能够根据市场需求及时调整培训课程内容，快速培养出企业急需的网络空间安全人才。然而，社会培训也存在一些局限性，如培训质量参差不齐，部分培训机构为追求经济效益，过度压缩培训时间，导致培训效果不佳。此外，社会培训的学员在理论知识的系统性方面相对薄弱，缺乏高校教育所提供的综合素质培养。

3.2 人才需求情况

3.2.1 不同行业企业对网络空间安全人才的需求数量与岗位分布

不同行业企业对网络空间安全人才的需求数量存在差异。根据本次调研数据，金融行业和互联网行业对网络空间安全人才的需求最为旺盛，分别占总需求的35%和30%。能源行业和政府部门的需求占比分别为20%和15%。在岗位分布方面，安全工程师岗位的需求占比最高，达到40%，主要负责企业网络安全防护体系的设计、建设和维护；安全分析师岗位需求占比为25%，主要从事网络安全威胁分析、风险评估等工作；安全运维人员岗位需求占比为

20%，负责网络安全设备的日常运维和管理；此外，安全架构师、安全合规官等岗位也有一定的需求。

3.2.2 人才需求的地域分布特点

网络空间安全人才需求在不同地区存在明显差异。东部沿海地区和一线城市由于经济发达，互联网、金融等行业集中，对网络空间安全人才的需求最为旺盛。例如，北京、上海、深圳等城市的网络空间安全人才需求量占全国总需求量的50%以上。中西部地区的人才需求相对较少，但随着中西部地区数字经济的发展，对网络空间安全人才的需求也在逐渐增加。造成这种地域差异的主要原因是经济发展水平和产业结构的不同，经济发达地区的企业对网络安全的重视程度更高，投入也更大，因此对人才的需求也更为迫切。

辽宁省的情况，根据前瞻产业研究院《2024-2029 年辽宁省信息安全市场前瞻与投资战略规划分析报告》，辽宁省信息安全市场规模持续扩大，2024 年依托数据安全法规强制实施市场规模为 68-72 亿元，到 2026 年收到工业互联网安全平台建成驱动市场规模预计能达到 90-98 亿元，2029 年市场规模更是能达到 130-145 亿元。2023 年网络安全人才缺口已达 11 万人（需求 59 万人，实际供给 48 万人）。随着数字辽宁、智造强省战略推进，预计到 2027 年缺口将进一步扩大，特别是工业互联网、关键信息基础设施防护等领域需求迫切。

3.3 人才供需匹配存在的问题

高校培养的人才在知识结构、实践能力、职业素养等方面与企业需求存在一定差距。在知识结构方面，高校教学内容更新相对滞后，对新兴技术如人工智能安全、量子计算安全等方面的知识传授不足，导致学生的知识结构无法满足企业对复合型人才的需求。实践能力方面，由于高校实践教学环节的局限性，学生缺乏实际项目经验，在解决实际网络安全问题时能力不足。职业素养方面，部分高校学生缺乏对网络安全行业的深刻理解，职业道德意识淡薄，在工作中可能出现违规操作等问题。

企业招聘过程中面临着高端技术人才匮乏、复合型人才不足等问题。高端技术人才方面，如能够掌握前沿网络安全技术、具备创新能力的人才供不应求，企业在招聘此类人才时往往面临激烈竞争。复合型人才方面，既懂网络安全技术，又了解行业业务的人才短缺，导致企业在网络安全与业务融合方面进展缓慢。例如，在金融行业，既熟悉金融业务流程，又具备网络安全专业知识的人才稀缺，难以满足金融机构对数字化转型过程中网络安全保障的需求。

四、未来行业产业对网络空间安全人才的新要求

4.1 物联网与工业互联网安全

物联网和工业互联网的网络架构具有设备数量庞大、通信协议复杂、安全防护薄弱等特点。据 Gartner 预测，到 2025 年，全球物联网设备连接数量将达到 250 亿，工业互联网市场规模将达到 1.5 万亿美元。如此庞大的设备连接数量和市场规模，使得物联网和工业互联网面

临着严峻的安全挑战。外部攻击方面，物联网设备易成为黑客攻击的目标，一旦被入侵，可能导致用户隐私泄露、设备失控等问题。工业互联网则面临着生产控制系统被攻击的风险，可能影响工业生产的正常进行，甚至造成重大安全事故。内部安全风险方面，物联网和工业互联网中的设备管理、人员操作等环节存在安全隐患，如设备密码设置简单、内部人员违规操作等。为应对这些安全风险，需要人才具备物联网和工业互联网安全防护技术能力。在设备安全方面，能够对物联网设备进行安全评估和加固，提高设备的安全性。在网络通信安全方面，掌握加密技术、安全路由等技术，保障数据在传输过程中的安全。在工业控制系统安全方面，熟悉工业控制系统的架构和运行原理，能够制定有效的安全防护策略。例如，Ponemon Institute 的研究报告指出，具备工业互联网安全专业知识的人才严重短缺，约 70%的企业表示难以招聘到合适的工业互联网安全人才。预计到 2028 年，物联网与工业互联网安全领域的人才需求将增长 80%，人才缺口将超过 50 万。培养适应物联网和工业互联网安全需求的专业人才迫在眉睫。

4.2 传统行业数字化转型对人才知识能力的新需求

传统制造业正加速推进数字化转型，据德勤《2024 年全球制造业转型报告》指出，全球 65%的制造企业已将数字化转型作为核心战略。在转型过程中，制造业引入了工业互联网平台、智能制造系统等，使得网络安全边界不断扩大，安全风险点增多。例如，生产设备与互联网的连接可能导致工业控制系统遭受远程攻击，影响生产进度和产品质量。这就要求网络空间安全人才具备跨学科知识，既要掌握网络安全技术，又要了解制造业的生产流程和工艺特点。能够针对制造业数字化系统，如 MES（制造执行系统）、ERP（企业资源计划）系统等，制定全面的安全防护策略，包括对生产数据的加密传输、访问权限的精细化管理等。

五、基于行业需求的网络空间安全专业人才培养

5.1 优化人才培养方案

5.1.1 明确培养目标与定位

结合行业对网络空间安全人才的迫切需求以及不同我校的自身特点，精准定位人才培养目标。我校将培养重点放在应用型人才上，立足行业需求与区域发展，聚焦“工控安全与行业数据防护”方向，培养兼具网络安全技术能力与行业应用视野的复合型人才。

我校网络空间安全专业面向国家网络安全战略需求与东北老工业基地数字化转型需要，围绕应用型人才培养定位及区域工业企业安全防护需求，培养德智体美劳全面发展的应用型技术人才。学生能够适应地方产业网络安全技术岗位需要，掌握网络攻防技术、工控安全原理、数据安全治理等基础理论，具备网络安全漏洞检测、安全运维、应急响应能力以及中小型企业安全方案实施能力，具有工匠精神、安全责任意识和团队协作素质。学生毕业后可在智能制造、能源化工、通信电子等工业企业，以及地方网信部门、安全服务机构从事网络安全运维、工控系统防护、数据安全治理、合规审计等工作。

5.1.2 完善课程体系设置

我校网络空间安全专业课程体系以数据通信及网络安全为核心主线，构建起层次清晰、特色鲜明的课程架构。在数据通信主线中，开设路由与交换原理与技术等课程，夯实学生对数据传输协议和网络架构的认知；网络安全主线则通过网络安全技术、网络攻防技术、渗透测试技术等课程，系统传授加密技术、入侵检测等核心安全能力。同时，课程体系突出工业控制与物联网安全特色，设置工控安全原理、工业控制与物联网安全、工业数据安全与合规等针对性课程，结合工业场景中的典型案例，让学生掌握工业控制网络的脆弱性分析、物联网设备固件安全检测等专项技能，形成“基础理论+行业特色+实战能力”的培养闭环。

5.2 加快教学内容迭代更新

建立教学内容动态更新机制，成立由我校教师、企业网络安全专家组成的教学内容更新委员会，每学年对教学内容进行评估和更新。及时将行业最新技术、安全事件案例、法律法规政策等纳入教学内容。

鼓励教师参与行业实践和学术研究，规定教师每年至少有 1 个月的时间参与企业实际网络安全项目或参加国内外学术会议。将教师的科研成果转化为教学内容，如将教师在工控网络安全方面的研究成果融入工业控制与物联网安全课程的教学中，丰富教学案例。

加强教材建设，组织教师与企业专家共同编写教材，教材内容要紧跟行业发展动态，体现时代特色，突出学校特色。

5.3 强化学生实习实践

5.3.1 加强实习基地建设

拓展与行业企业的合作，力争至少与 10 家不同行业的企业建立稳定的实习基地，其中包括大型互联网企业、金融机构、能源企业和政府部门合作单位等。实习基地具备相应的实习条件和指导人员。

加强与实习基地的沟通与协作，每学期与实习基地共同制定实习计划，明确实习任务与要求。在互联网企业的实习中，让学生参与网站的安全防护工作。定期对实习效果进行评估，根据评估结果调整实习计划，确保实习质量。

5.3.2 设计多样化实践项目

结合行业实际需求，设计综合性、创新性的实践项目。在高年级每学期至少安排 1 个大型综合实践项目，如网络安全攻防演练项目，模拟企业真实的网络环境，让学生扮演攻击方和防御方进行实战演练；安全系统设计与开发项目，让学生根据特定行

业的需求设计并开发网络安全防护系统；安全风险评估项目，组织学生对学校或合作企业的网络系统进行风险评估并提出改进方案。

鼓励学生参与各类网络空间安全竞赛，如全国大学生信息安全竞赛、各类网络攻防大赛等。学校为参赛学生提供专业的指导和培训，设立竞赛奖励基金，对获奖学生给予表彰和奖励。通过竞赛能有效提升学生的实践能力和创新能力。

5.3.3 完善实践教学评价体系

建立科学合理的实践教学评价指标体系，从实践项目完成情况、学生实践能力提升、实习单位评价等多个方面进行综合评价。加强对实践教学过程的监督与管理，安排专人负责实践教学的日常管理工作，定期检查实践教学的进展情况，及时发现问题并进行整改。建立实践教学档案，记录学生的实践过程和评价结果，为学生的学分认定和就业推荐提供依据。

5.4 加强师资队伍建设

加大网络空间安全专业教师的引进力度，制定优惠政策吸引具有丰富行业实践经验和新兴技术背景的人才加入教师队伍。优先引进具有 CISSP、CISA 等国际权威网络安全认证证书的人才，以及在云计算安全、人工智能安全等新兴领域有深入研究的专业人才。

鼓励教师参加行业培训、学术交流活动，学校每年为每位教师提供不少于 2 次的行业培训或学术交流机会。支持教师参加国内外高水平的网络安全学术会议，了解行业最新动态和前沿技术，提升教师的专业素养和实践能力。

建立教师企业挂职锻炼制度，教师每 3 年至少有 6 个月的时间到企业挂职锻炼，参与企业的实际网络安全项目。与合作企业签订挂职锻炼协议，明确双方的权利和义务，企业为挂职教师提供必要的工作条件和指导，学校将教师的挂职锻炼经历纳入职称评聘和绩效考核的重要内容，以激励教师积极参与企业实践，丰富教学案例。

六、结论与展望

6.1 调研结论

本次调研围绕网络空间安全行业产业人才需求展开，系统梳理了行业发展现状、人才供需格局及未来需求趋势，为沈阳化工大学新增网络空间安全专业的人才培养提供了明确依据。当前网络空间安全市场呈现高速增长态势，2024 年全球市场规模达 233.4 亿美元，其中工业控制、物联网等领域的安全需求尤为突出，全球工业领域网络攻击事件较 2020 年增长 187%，而辽宁省作为东北老工业基地，2023 年网络安全人

才缺口已达 11 万人，且随着“数字辽宁、智造强省”战略推进，工业互联网安全人才需求将持续扩大。

从人才供需来看，高校培养规模与行业需求存在显著错配：全国年毕业 1.5 万余人但区域供给不足（辽宁年均培养不足 400 人），且现有人才在知识结构（新兴技术覆盖不足）、实践能力（缺乏工业场景经验）、复合素养（行业知识融合不够）等方面与企业需求存在差距。特别是工业控制、能源化工等领域，既懂网络安全技术又熟悉工业生产流程的复合型人才稀缺，很多企业面临工控安全人才招聘困难。

沈阳化工大学将网络空间安全专业定位为“工控安全与行业数据防护”方向，构建“数据通信+网络安全”双主线课程体系，突出工业控制与物联网安全特色，通过校企协同、实践导向的培养模式，培养适应区域产业需求的应用型人才，这一定位既契合国家网络安全战略，又精准对接东北老工业基地数字化转型的迫切需求。

6.2 未来展望

从行业发展看，随着工业互联网、人工智能、量子计算等技术的深度应用，网络安全的内涵与外延将持续拓展。预计到 2028 年，物联网与工业互联网安全领域人才需求将增长 80%，人才缺口超 50 万，其中具备跨学科能力的复合型人才、掌握前沿技术的创新型人才将成为行业争夺的核心资源。辽宁省信息安全市场规模预计 2029 年达 130-145 亿元，工业控制系统防护、数据安全治理等领域的人才需求将呈现爆发式增长。

对沈阳化工大学而言，未来重点推进三方面工作：一是动态优化课程体系，紧跟工业协议安全、量子抗攻击等技术发展，每学年更新一定比例的教学内容；二是深化校企协同育人，扩大实习基地至 15 家以上，覆盖能源化工、智能制造等特色产业，建立“企业项目进校园”机制；三是构建区域人才生态，联合政府、企业打造“培训-竞赛-就业”链条，力争 3-5 年内成为东北工业安全人才培养的核心基地。

长远来看，网络空间安全人才培养需突破“技术孤岛”思维，向“技术+行业+法规”深度融合演进。学校应持续跟踪《网络安全法》《数据安全法》等法规更新，强化学生合规意识；通过参与“熵密杯”“工控安全挑战赛”等赛事提升实战能力，最终实现培养一批“能扎根东北、服务工业、懂安全防护”的高素质人才，为区域产业安全发展和国家网络空间安全战略提供坚实支撑。

5. 申请增设专业人才培养方案

沈阳化工大学本科培养方案

计算机科学与技术学院

专业名称：网络空间安全

专业代码：080911TK

制　　定：王翠青

审　　核：张　波

审　　定：王　娜

批　　准：于三三

2025 年 7 月

网络空间安全专业培养方案

一、专业介绍

网络空间安全专业立足行业需求与区域发展，聚焦“工控安全与行业数据防护”方向，培养兼具网络安全技术能力与行业应用视野的复合型人才。

专业面向国家网络安全战略与东北老工业基地数字化转型需求，以“行业赋能、实战驱动”为核心定位，重点培养化工、能源等工业领域网络安全防护人才，强化工业控制系统安全、数据安全治理、智能安全分析等特色方向。

专业整合网络工程（网络攻防技术）、数据科学（大数据隐私保护）、计算机科学（系统安全架构）等学科资源，构建“安全技术+行业场景”课程体系，开设《业控制与物联网安全》《化工数据安全与合规》等特色课程。与安恒信息、沈阳网信办共建“工业安全联合实验室”，开展工控漏洞挖掘、工业数据脱敏等实践项目，形成“教学-实训-就业”一体化培养链。

专业依托辽宁省工业数字化转型需求，聚焦化工生产场景中的网络威胁监测与应急响应，为东北地区工业互联网安全提供人才与技术支撑。

二、培养目标

本专业面向国家网络安全战略需求与东北老工业基地数字化转型需要，围绕应用型人才培养定位及区域工业企业安全防护需求，培养德智体美劳全面发展，适应地方产业网络安全技术岗位需要，掌握网络攻防技术、工控安全原理、数据安全治理等基础理论，具备网络安全漏洞检测、安全运维、应急响应能力以及中小型企业安全方案实施能力，具有工匠精神、安全责任意识和团队协作素质，毕业后可在智能制造、能源化工、通信电子等工业企业，以及地方网信部门、安全服务机构从事网络安全运维、工控系统防护、数据安全治理、合规审计等工作的高素质应用型技术人才。

通过校企联合培养与典型工业场景实战训练，毕业生能够快速融入区域产业一线岗位，解决工业生产、能源传输等场景中的网络威胁监测、数据隐私保护等实际问题，为东北地区工业数字化转型提供可靠的安全技术支撑，成为“懂技术、重实践、能扎根”的基层网络安全骨干力量。

本专业毕业生具有如下目标预测：

培养目标 1:工程知识与解决问题能力：毕业生能够系统掌握网络协议分析、密码学基础、工业控制系统架构等核心知识，融合安全防护技术原理，精准识别化工、能源等工业场景中的网络威胁，具备独立解决工控网络入侵检测、数据泄露溯源、安全策略优化等实际工程问题的能力。

培养目标 2:工程设计与创新能力：能够针对工业互联网、智能制造的特定需求，设计可行的网络安全防护方案，并融合 AI、区块链等新技术提出创新性安全优化策略，参与企业级安全系统升级或科研项目研发，形成专利、技术报告等成果。

培养目标 3:伦理责任与社会意识：深刻理解网络安全法律法规和职业道德规范，在工程实践中恪守

数据隐私保护原则，主动规避技术滥用风险，具备应对“数据利用与隐私保护”“安全效率与合规成本”等伦理挑战的决策能力，为区域工业安全可持续发展贡献力量。

培养目标 4:沟通协作与领导力：能够在跨学科团队中清晰表达技术方案，协同完成工业安全运维、应急响应等任务，通过参与 CTF 竞赛、校企联合攻防演练等项目积累协作经验；工作 5 年内可成长为中小型项目负责人，统筹协调资源，制定安全实施计划，并具备向客户、管理层传递技术价值的沟通能力。

培养目标 5:终身学习与职业发展：主动跟踪云安全、隐私计算等前沿技术动态，通过 CISP、CISA 等认证或行业培训持续提升专业水平；适应网络安全领域快速迭代的特性，制定清晰的职业规划，逐步从技术实施岗位向安全管理、合规咨询等复合型角色拓展，具备应对行业变革与技术转型的韧性。

三、专业方向

网络空间安全，工业互联网安全

四、毕业要求及实现矩阵

本专业毕业生在毕业时，应该具备较强的社会责任感和基本人文素养；理解与掌握数学、自然科学和计算机科学的理论知识；理解和掌握复杂网络空间安全领域的规划与设计原理、应用系统开发流程、网络安全实施的原理等知识，接受科学思维和科学实验的基本训练；接受从事研究与应用网络空间安全的基本训练，在网络安全运维、工控系统防护、数据安全治理方面具有较宽的工程技术基础和一定的专业知识。具有较强的相关技术处理能力和一定的系统分析能力，了解本专业的发展方向和最新成就，具有较强的自学能力和不断更新知识的能力，较熟练掌握一门外语。

毕业能力要求及其指标点分解：

毕业能力要求	指标点
0.立德树人： 具有坚定正确的政治方向、良好的思想品德和健全的人格，热爱祖国，热爱人民，拥护中国共产党的领导；具有科学精神、人文修养、职业素养、社会责任感和积极向上的人生态度，了解国情社情民情，践行社会主义核心价值观。	0.1 坚定拥护党的领导，热爱祖国，具备良好的思想品德与人文素养
	0.2 弘扬科学精神与工匠精神，保持积极进取的人生态度
	0.3 立足国情社情，运用历史与哲学方法分析社会现象，践行社会主义核心价值观
1.工程知识： 掌握本专业所需的数学、自然科学、计算、工程基础和计算机科学知识，并能够用于解决复杂网络空间安全问题。	1.1 运用数学建模与逻辑分析方法，解析网络系统运行机理及安全威胁演化规律
	1.2 掌握计算机体系结构、算法设计与网络协议原理，支撑安全系统的开发与优化
	1.3 融合密码学、网络攻防等专业知识，完成工业级安全架构设计与风险评估
2.问题分析： 能够应用数学、自然科学和计算机科学的第一性原理，识别、表达、并通过文献研究分析辅助网络空间安全问题，综合考虑可持续发展的要求，以获得有效结论。	2.1 运用数学与计算机科学原理，精准定位工控漏洞、数据泄露等安全问题
	2.2 结合环境、经济与社会效益，评估安全策略的长期影响与可行性
	2.3 通过文献研究与威胁建模，构建符合行业规范的系统性应对方

	案
3. 设计解决方案： 能够针对复杂网络空间安全问题开发和设计解决方案，设计满足网络系统设计、部件选择、工程实施流程，体现创新性，并从健康与安全、全生命周期成本与净零碳要求、法律与伦理、社会与文化等角度考虑可行性。	3.1 掌握零信任架构、隐私计算等技术，制定分级防护策略与实施路径
	3.2 根据行业场景需求，完成安全模块选型、系统集成与工程部署
	3.3 综合考虑全生命周期成本、法律合规与社会文化因素，优化技术方案
4. 研究： 能够基于科学原理并采用科学方法对复杂网络空间安全问题进行研究，包括设计实验、分析与解释数据、并通过信息综合得到合理有效的结论	4.1 设计实验方案验证安全技术有效性（如漏洞挖掘、攻击检测）
	4.2 通过数据采集与分析构建安全模型，提炼关键结论
	4.3 输出符合学术规范或工程标准的研究报告与改进建议
5. 使用现代工具： 能够针对复杂网络空间安全问题，开发、选择与使用恰当的技术、资源、现代工程工具和信息技术工具，包括对复杂工程问题的预测与模拟，并能够理解其局限性	5.1 运用渗透测试、流量分析等工具开展安全评估与取证
	5.2 通过仿真平台模拟网络环境，验证防护方案可靠性
	5.3 开发定制化工具解决特定场景下的安全技术瓶颈
6. 工程与可持续发展： 在解决复杂网络空间安全问题时，能够基于专业相关背景知识，分析和评价网络空间安全实践对健康、安全、环境、法律以及经济和社会可持续发展的影响，并理解应承担的责任。	6.1 评估安全方案对环境保护、能源消耗及区域产业升级的贡献度
	6.2 遵循国家法律法规设计等保合规实施方案
	6.3 制定兼顾技术可行性与社会效益的渐进式改造计划
7. 伦理和职业规范： 有网络技术报国、网络技术为民的意识，具有人文社会科学素养和社会责任感，能够理解和应用网络技术伦理，在网络空间安全实践中遵守工程职业道德、规范和相关法律，履行责任。	7.1 在渗透测试、数据治理中严守法律边界与职业道德
	7.2 制定行业场景化安全责任管理制度
	7.3 参与网络安全科普，提升公众数字素养
8. 个人和团队： 能够在多样化、多学科背景下的团队中承担个体、团队成员以及负责人的角色。	8.1 在团队中明确角色分工，协同完成攻防演练、安全加固等项目
	8.2 协调技术、管理与客户需求，推动方案落地实施
	8.3 领导小组完成区域性关键设施安全评估任务
9. 沟通： 能够就复杂网络空间安全问题与业界同行及社会公众进行有效沟通和交流，包括撰写报告和设计文稿、陈述发言、清晰表达或回应指令；能够在跨文化背景下进行沟通和交流，理解、尊重语言和文化差异。	9.1 编制符合国际标准的技术文档与实施方案
	9.2 向非技术人员解读安全风险与防护价值
	9.3 阅读外文文献并参与国际技术交流
10. 项目管理： 理解并掌握复杂网络空间安全项目相关的管理原理与经济决策方法，并能在多学科环境中应用。	10.1 运用项目管理工具制定进度计划与风险预案法
	10.2 基于成本效益分析优化资源配置
	10.3 统筹多部门协作完成大型安全改造项目
11. 终身学习：	11.1 通过认证培训掌握前沿技术（如云安全、AI 攻防）

具有自主学习和终身学习的意识和能力，能够理解广泛的技术变革对网络空间安全专业和社会的影响，适应新技术变革，具有批判性思维能力。	11.2 构建系统性知识框架应对新型网络威胁
	11.3 参与行业论坛跟踪技术演进与政策动向

毕业要求支撑培养目标实现的关系矩阵

毕业要求	培养目标				
	培养目标 1	培养目标 2	培养目标 3	培养目标 4	培养目标 5
0：立德树人			√		
1：相关（工程）知识	√				
2：问题分析	√				
3：设计/开发解决方案		√			
4：研究		√			√
5：使用现代工具	√				
6：专业（工程）与可持续发展			√		
7：伦理和职业规范			√		
8：个人和团队				√	
9：沟通				√	√
10：项目管理		√		√	
11：终身学习					√

四、主干学科与交叉学科

主干学科：网络空间安全

五、专业核心课程

计算机网络、网络空间安全导论、网络安全技术、软件安全、Web应用安全、渗透测试技术、工业控制与物联网安全、网络攻防技术、网络空间安全专业实践

六、学制与学位

学制：基本学制4年，弹性修业年限3-6年。

毕业要求总学分：160学分

授予学位：符合国家学位规定和《沈阳化工大学本科毕业生学士学位授予工作有关规定(2017 年 3 月修订)》学位授予条件者，授予工学学士学位。

七、学分要求

<table>
<tr><th>培养环节</th><th>课程性质</th><th>课程类别</th><th>课程模块</th><th>学分要求</th><th>小计</th></tr>
<tr><td rowspan="23">课内环节</td><td rowspan="10">必修</td><td rowspan="7">通识教育课程</td><td>思政类</td><td>17</td><td rowspan="7">39</td></tr>
<tr><td>外语类</td><td>10</td></tr>
<tr><td>军事安全类</td><td>2</td></tr>
<tr><td>劳动体育类</td><td>5</td></tr>
<tr><td>创新创业类</td><td>2</td></tr>
<tr><td>心理健康类</td><td>1</td></tr>
<tr><td>人工智能类</td><td>2</td></tr>
<tr><td rowspan="3">学科基础课程</td><td>数学与自然科学类</td><td>24</td><td rowspan="3">55.5</td></tr>
<tr><td>工程基础类</td><td>4</td></tr>
<tr><td>专业基础类</td><td>29.5</td></tr>
<tr><td rowspan="9">选修</td><td rowspan="6">通识教育课程</td><td>美育类(400)</td><td>2</td><td rowspan="6">10</td></tr>
<tr><td>中国与世界(500)</td><td>1</td></tr>
<tr><td>四史(600)</td><td>1</td></tr>
<tr><td>经济管理类(700)</td><td>2</td></tr>
<tr><td>科技前沿类(800)</td><td>2</td></tr>
<tr><td>优秀文化传承类（900）</td><td>2</td></tr>
<tr><td rowspan="3">专业教育课程</td><td>专业方向类</td><td>22</td><td rowspan="3">24</td></tr>
<tr><td>学科领域类</td><td>2</td></tr>
<tr><td>专业特色（拓展）类</td><td>4</td></tr>
<tr><td rowspan="4">实践</td><td rowspan="4">实践教育课程</td><td>通识教育实践类</td><td>2</td><td rowspan="4">31.5</td></tr>
<tr><td>学科基础实践类</td><td>3</td></tr>
<tr><td>专业实践类</td><td>22</td></tr>
<tr><td>专业特色（拓展）实践类</td><td>4.5</td></tr>
<tr><td rowspan="6">课外环节</td><td colspan="2" rowspan="2">课外通识实践</td><td>人文社会实践</td><td rowspan="2">2</td><td rowspan="6">不计入总学分</td></tr>
<tr><td>身心健康实践</td></tr>
<tr><td colspan="2" rowspan="3">创新创业实践</td><td>创新训练</td><td rowspan="3">4</td></tr>
<tr><td>创新大赛</td></tr>
<tr><td>创客活动</td></tr>
<tr><td colspan="2">生涯教育及成长规划类</td><td>职业规划与就业指导</td><td>1</td></tr>
<tr><td colspan="5">总学分</td><td>160</td></tr>
</table>

八、网络空间安全专业教学进程表

（1）必修课设置及学分分配表

课程类别 Course Type	课程模块 Course Nature	序号 No.	课程号 Course Code	课程名称 Course Name	学分 Cre.	总学时数 Total Cre.	学时分配 Credit Hour Distribution 讲课 Lec.	实验 Exp.	上机 Pro.	课外实践 Pra.	开课学期 Semester	备注 Notes
通识教育课程 General Education	思政类 Ideological & Political	1	0710093001	思想道德与法治 ‖ Ideology & Morality and Rule of Law	3.0	48	32			16	1	
		2	0710053001	中国近现代史纲要 ‖Outline of Chinese Contemporary and Modern History	3.0	48	32			16	2	
		3	0710043001	马克思主义基本原理* ‖Basic Principle of Marxis*	3.0	48	32			16	3	
		4	0710133001	毛泽东思想和中国特色社会主义理论体系概论* ‖Mao Zedong Thought and Theory of Socialism with Chinese Characteristics *	3.0	48	32			16	4	
		5	0710123001	习近平新时代中国特色社会主义思想概论 ‖Introduction to Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era	3.0	48	40			8	5	
		6	0710012301	形势与政策 ‖Current Situation and Policies	2.0	64	64				1～8	第 8 学期记学分
	外语类 Foreign Language	7	0211003101	大学外语Ⅰ ‖College EnglishⅠ	3.0	48					1	
		8	0211003201	大学外语Ⅱ* ‖College English Ⅱ*	3.0	48					2	
		9	0241003301	大学外语Ⅲ ‖College English Ⅲ	2.0	32					3	
		10	0241003401	大学外语Ⅳ* ‖College EnglishⅣ*	2.0	32					4	
	人工智能类 AI	11	1616222001	人工智能导论 ‖ Introduction to Artificial	2.0						3	

				Intelligence								
	军事安全类 Military & Safety	12	0710081001	军事理论 ‖Military Theory	1.0	16					1	
		13	1618041001	安全教育 ‖Safety Education	1.0	16					1	
通识教育课程 General Education	劳动体育类 Labor & Sport Education	14	2640021001	劳动教育 ‖Labour Education	1.0	16	16				1	
		15	0410011101	大学体育Ⅰ ‖College Physical EducationⅠ	1.0	36		36			1	
		16	0410021201	大学体育Ⅱ ‖College Physical EducationⅡ	1.0	36		36			2	
		17	0410031301	大学体育Ⅲ ‖College Physical EducationⅢ	1.0	36		36			3	
		18	0410041401	大学体育 Ⅳ ‖College Physical Education Ⅳ	1.0	36		36			4	
	创新创业类 Innovation & Entrepreneurship	19	1617021002	创造性思维与创新方法 ‖Creative Thinking and Innovative Methods	1.0						3	
		20	1740011001	创业基础 ‖Entrepreneurial Foundation	1.0	16	16				4	
	心理健康类 Mental & Health	21	0510041001	大学生心理与健康教育 ‖Mental and Health Education for College Students	1.0	16	16				1	
合计 Subtotal					39.0							
学科基础课程 Discipline Education	数学与自然科学类 Natural Science & Mathematics	22	0310004101	高等数学 I* ‖Advanced Mathematics I*	4.5	80	72			8	1	
		23	0310005201	高等数学 II* ‖Advanced Mathematics II*	5.5	96	88			8	2	
		24	1617052002	离散数学 ‖Discrete Mathematics	3.0	48	48				2	
		25	0310063201	大学物理* ‖University Physics	3.0	48	48				2	
		26	0310034001	线性代数 ‖Linear Algebra	4.0	64	64				3	
		27	1637232002	网络空间安全数学基础 ‖Mathematical Foundations of Cybersecurity	2.0	32	32				3	
		28	0317184001	概率论与数理统计 ‖Probability and Statistics	2.0	32	32				4	
	工程基础类 Foundation Engineering	29	1610052002	计算机科学导论 ‖Introduction to Computer Science	2.0	32	32				1	
		30	1612021002	工程导论 ‖Introduction to Engineering	1.0	16	16				1	

<table>
<tr><td rowspan="14"></td><td rowspan="2"></td><td>31</td><td>1612051002</td><td>专业外语与文献检索及写作 ||Document Retrieval and Scientific Paper Writing</td><td>1.0</td><td>16</td><td>16</td><td></td><td></td><td></td><td>6</td><td></td></tr>
<tr><td>32</td><td>1637041002</td><td>网络安全法律法规 ||Cybersecurity Laws and Regulations</td><td>1.0</td><td>16</td><td>16</td><td></td><td></td><td></td><td>5</td><td></td></tr>
<tr><td rowspan="12">专业基础类 Subject Foundation Requisite</td><td>33</td><td>1644270002</td><td>学业与专业教育 ||Academic and Professional Education</td><td>0.5</td><td>8</td><td>8</td><td></td><td></td><td></td><td>1</td><td></td></tr>
<tr><td>35</td><td>1610043102</td><td>C 语言程序设计* ||C Programming Language*</td><td>3.0</td><td>56</td><td>32</td><td></td><td>24</td><td></td><td>1</td><td></td></tr>
<tr><td>36</td><td>1610083002</td><td>算法与数据结构* ||Algorithm and Data Structures*</td><td>3.0</td><td>52</td><td>40</td><td></td><td>12</td><td></td><td>2</td><td></td></tr>
<tr><td>37</td><td>1610073002</td><td>面向对象程序设计 ||Object-Oriented Programming</td><td>2.5</td><td>44</td><td>32</td><td></td><td>12</td><td></td><td>2</td><td></td></tr>
<tr><td>38</td><td>1610243002</td><td>数字逻辑与 EDA 技术 ||Digital Logic and EDA Technology</td><td>2.0</td><td>36</td><td>24</td><td>12</td><td></td><td></td><td>3</td><td></td></tr>
<tr><td>39</td><td>1637032002</td><td>网络空间安全导论 ||Introduction to Cybersecurity</td><td>2</td><td>32</td><td>32</td><td></td><td></td><td></td><td>3</td><td></td></tr>
<tr><td>40</td><td>1610093002</td><td>计算机组成原理* ||Computer Organization and Architecture*</td><td>3.0</td><td>52</td><td>40</td><td>12</td><td></td><td></td><td>4</td><td></td></tr>
<tr><td>41</td><td>1610123002</td><td>数据库系统原理及安全 ||Principles and Security of Database Systems</td><td>3.0</td><td>52</td><td>40</td><td></td><td>12</td><td></td><td>4</td><td></td></tr>
<tr><td>42</td><td>1637071002</td><td>信息存储技术 ||Information Storage Technology</td><td>1.5</td><td>24</td><td></td><td></td><td></td><td></td><td>4</td><td></td></tr>
<tr><td>43</td><td>1610142002</td><td>计算机网络* ||Computer Networking*</td><td>3.0</td><td>52</td><td>40</td><td></td><td>12</td><td></td><td>3</td><td></td></tr>
<tr><td>44</td><td>1614332002</td><td>操作系统原理及安全 ||Operating Systems and Security</td><td>3.0</td><td>48</td><td>48</td><td></td><td></td><td></td><td>5</td><td></td></tr>
<tr><td colspan="5">合计 Subtotal</td><td>55.5</td><td>936</td><td>800</td><td>24</td><td>72</td><td></td><td></td><td></td></tr>
</table>

注：1.理论课 1 学分 16 学时，实验课程、上机等 1 学分 24 学时，体育课 1 学分 36 学时，集中实践环节 1 个教学周计 1 学分，学分最小单位为 0.5。

2.课程名称中带*为考试课。

（2）选修课设置及学分分配表

课程类别 Course Type	课程模块 Course Nature	序号 No.	课程号 Course Code	课程名称 Course Name	学分 Cre.	总学时数 Total Cre.	学时分配 Credit Hour Distribution				开课学期 Semester	备注 Notes
							讲课 Lec.	实验 Exp.	上机 Pro.	课外实践 Pra.		
通识教育课程 General Education	分为美育类、中国与世界、四史、经济管理类、科技前沿类、优秀文化传承类 6 个课程模块 每个模块最多选修 2 学分，每学期最多选修 1 门课程。 Including 6 modules: Aesthetic Education, China and The world, Four Histories, Economic Management,Frontier science and technology, Excellent cultural inheritance, . Up to 2 credits per module and up to 1 courses per semester.											
合计 Subtotal					10							
专业教育课程 Specialized Education	专业方向类 Orientation	45	1610082002	密码学基础 || Cryptography	2.0	32	32				3	
		46	1637093002	Web 应用开发 || Web Application Developmen	2.0	48	24		24		4	
		47	1637103002	Web 应用安全 ||Web Application Security	2.0	48	24		24		5	
		48	1610782002	网络安全技术* ||Network Security Technology	2.0	32	32				5	
		49	1637113002	渗透测试技术 ||Penetration Testing Techniques	2.0	32	32				5	
		50	1637143002	软件安全 ||Principles of Software Security	2.0	32	32				6	
		51	1637122002	大数据技术及安全 ||Big Data Technology and Security	2.0	40	16		24		5	
		52	1637132002	路由交换原理与技术 ||Principles and Technologies of Routing and Switching	2.0	32	32				4	
		53	1617182002	网络攻防技术 ||Network Attack and Defense Technologies	2.0	32	32				6	
		小计 Subtotal			18	328	256		72			
	学科领域类 Discipline	54	1610112002	编译原理 ||Compiler Construction Priciples	2.5	44	32		12		6	
		55	1634192002	移动互联网技术||Mobile	2.0	36	24	12			5	

				Internet Technology								
		56	1638002002	Python 语言||Python Language	2.0	40	16	24			6	
		57	1630462002	Java 语言程序设计 ||Java Programming	3.0	56	32		24		2	
		58	1637152002	信息通信基础 ||Fundamentals of Information and Communication	1.5	24	24				6	
	学科领域类 Discipline	59	1650752102	程序设计竞赛 I||Programming Competition I	2.5	48	24		24		3	
		60	1637162002	汇编语言程序设计 ||Assembly Language Programming	2.5	44	32		12		5	
		61	1637172002	工控安全原理 ||Principles of Industrial Control Security	2.0	32					6	
		62	1637172002	通信原理 ||Principles of Communications	3.0	52	40		12		5	
		63	1610152002	软件工程 ||Software Engineering	2.5	40	40				6	
		小计 Subtotal			21	372	264	36	84			
		至少修读 2 学分										
	专业特色（拓展）类 Specialty Characteristics or Competency Development	64	1610842002	工业控制与物联网安全 ||Industrial Control and IoT Security	2.0	40	16	24			6	
		65	1637182002	工业数据安全与合规 ||Industrial Data Security and Compliance	2.0	32	32				7	
		小计 Subtotal			4.0	72	48	24				
		至少修读 4 学分										
合计 Subtotal					45.5	816	536	60	156			

（3）实践环节设置及学分分配表

课程类别 Course Type	课程模块 Course Nature	课程号 Course Code	课程名称 Course Name	学分 Cre.	总学时数 Total Cre.	方式 App.	周数 Weeks	开课学期 Semester	备注 Notes
实践教育课程 Practice Education	通识教育实践类 Ideological and Political Courses	0415102011	军训 ||military training	2.0	48		+2	1	
	小计 Subtotal			2.0	48				
	学科基础实践类 Foreign Language Courses	0310081011	大学物理实验 ||College Physics Laboratory	1.0	24	分散	16	2	
		1637191002	操作系统原理与安全实践 ||Operating Systems and Security Practice	1.0	24	分散	8	5	
		1637201002	计算机网络实践 ||Practice of Computer Network	1.0	24	分散	8	4	
	小计 Subtotal			3.0	72				
	专业实践类 Labor and Sport Education	1610802022	路由和交换网络设计||Design of Routing and Switching Network	2.0	48	分散	8	5	
		1637222002	工业控制与物联网安全实践 ||Industrial Control and IoT Security Practices	2.0	48	分散	8	6	
		1637232002	网络安全攻防实训 ||Offensive and Defensive Cybersecurity Hands-on Training	2.0	48	分散	8	6	
		1618022002	网络安全协议分析||Analysis of Network Security Protocol	2.0	48	分散	8	6	
		1615232032	生产实习 ||Production Practice	2.0	48	集中	2	7	
		1617031042	毕业设计（论文）||Graduation Design（Thesis）	12.0	288	分散	16	8	
	小计 Subtotal			22.0	528				
	专业特色（拓展）实践类 Innovation and Entrepreneurship courses	1614251002	网络空间安全竞赛实践 ||Practice of Cybersecurity Competition	1.5	36	分散	8	6	
		1615283022	网络空间安全专业实践 ||Practice of Cybersecurity Professional	3.0	72	分散	8	7	
	小计 Subtotal			4.5	108				
合计 Subtotal				31.5					

（4）课外环节设置及学分分配表

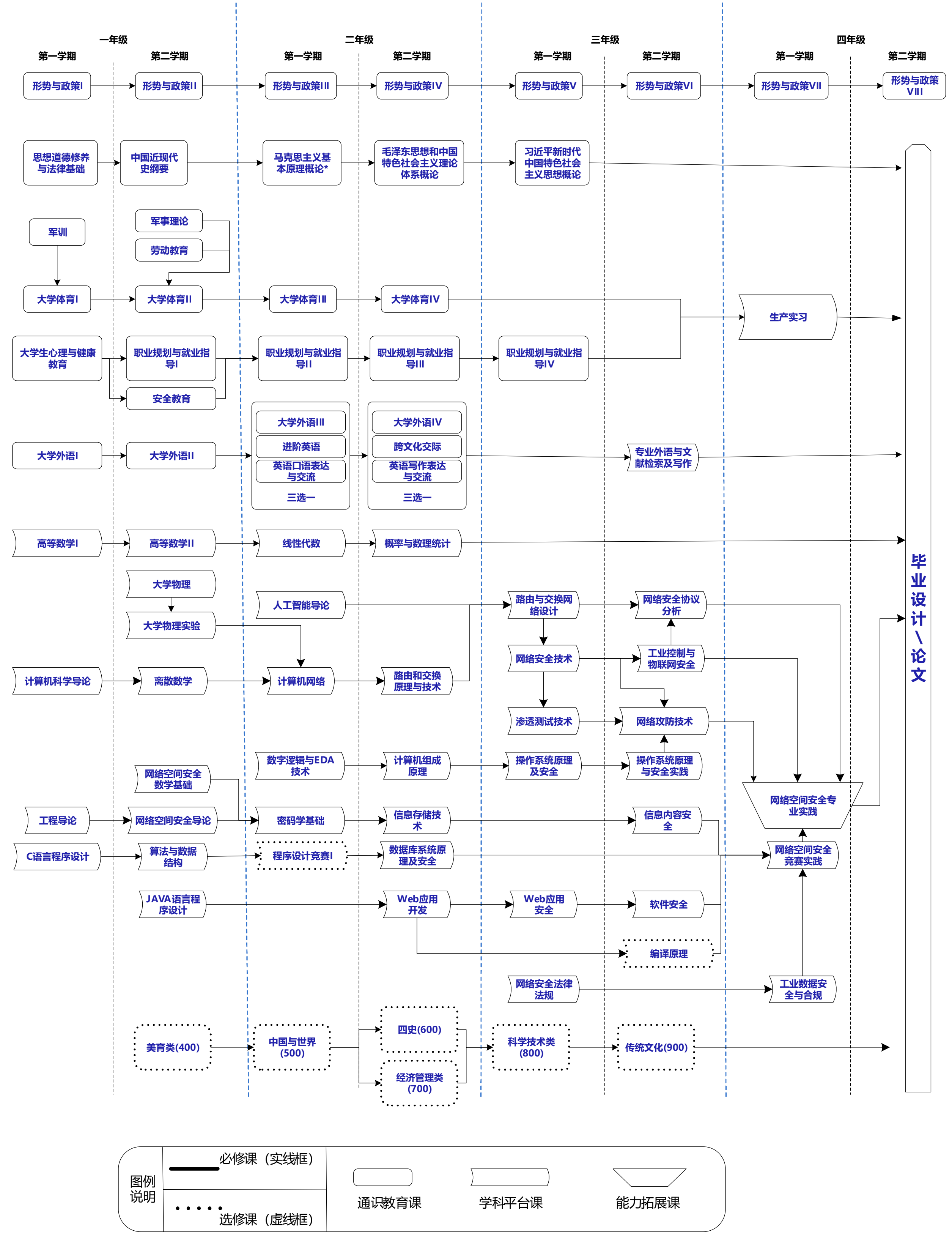
<table>
<tr><th>课程类别
Course Type</th><th>课程模块
Course Nature</th><th>课程号
Course Code</th><th>课程名称
Course Name</th><th>学分
Cre.</th><th>总学时数
Total Cre.</th><th>方式
App.</th><th>周数
Weeks</th><th>开课学期
Semester</th><th>备注
Notes</th></tr>
<tr><td rowspan="6">课外通识实践课程
Extracurricular General Education Practice</td><td>人文社会实践
Culture and Society Practice</td><td>0410120751</td><td>社会调查
||Social Survey</td><td>0.5</td><td>12</td><td>分散</td><td></td><td></td><td></td></tr>
<tr><td rowspan="3">身心健康社会实践
Mentally and Physically Practice</td><td>0410050751</td><td>课外体育锻炼
||Extracurricular Physical Exercise</td><td>0.5</td><td>12</td><td>分散</td><td></td><td></td><td></td></tr>
<tr><td>2640030011</td><td>劳动教育实践
||Labour Education Practice</td><td>0.5</td><td>12</td><td>分散</td><td></td><td></td><td></td></tr>
<tr><td>0510070311</td><td>心理健康辅导
||Mental Health Counseling</td><td>0.5</td><td>12</td><td>分散</td><td></td><td></td><td></td></tr>
<tr><td>能力与创新实践
Capability and Innovation Practice</td><td>0410130751</td><td>大学生素质拓展与创新实践
||Quality Development and Innovation Practice</td><td>4.0</td><td>96</td><td>分散</td><td colspan="3">1～8 学期依据《沈阳化工大学创新创业实践学分认定办法》由创新创业学院认定</td></tr>
<tr><td>生涯教育及成长规划类
Career Education and Growth Plan</td><td>0410130751</td><td>职业规划与就业指导
||Career Planning and Employment Guidance</td><td>1.0</td><td>40</td><td>分散</td><td></td><td></td><td></td></tr>
<tr><td colspan="4">合计 Subtotal</td><td>7.0</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

九、网络空间安全专业学士学位课程一览表
A list of bachelor's degree programs in Cyberspace Security

课程类别 Course Type	模块名称 Modules	序号 No.	课程编号 Course Codes	课程名称 Course Name	学分 Credits	开课学期 Semester
通识教育课 General Education	思政类 Ideological and Political	1	0710043001	马克思主义基本原理 ||Basic Principle of Marxis	3.0	3
		2	0710133001	毛泽东思想和中国特色社会主义理论体系概论 ||Mao Zedong Thought and Theory of Socialism with Chinese Characteristics	3.0	4
学科平台课 Discipline Education	学科基础类 Foundation Engineering"	3	0310004101	高等数学I Advanced Mathematics I	4.5	1
		4	0310005201	高等数学II Advanced Mathematics II	5.5	2
	专业基础类 Subject Foundation Requisite	5	1617052002	离散数学 ||Discrete Mathematics	3.0	2
		6	1610043102	C 语言程序设计 ||C Language Programming	3.0	1
		7	1610083002	算法与数据结构 ||Algorithm and Data Structure	3.0	2
		8	1610093002	计算机组成原理 ||Computer Organization and Architecture	3.0	4
		9	1610142002	计算机网络 ||Computer Networking	3.0	3
		10	1614332002	操作系统原理及安全 ||Operating Systems and Security	3.0	5
专业教育课 Specialized Education		11	1637103002	Web 应用安全 ||Web Application Security	3.0	5
		12	1610782002	网络安全技术 ||Network Security Technology	2.5	5
		13	1610842002	工业控制与物联网安全 ||Industrial Control and IoT Security	2.0	6
		14	1617182002	网络攻防技术 ||Network Attack and Defense Technologies	2	6

说明：关于学士学位课的具体要求见《沈阳化工大学关于学士学位课程水平审核制度的若干规定》

十、课程体系配置图 Curriculum System Configuration Diagram



6.教师及课程基本情况表

6.1专业核心课程情况表

课程名称	课程总学时	课程周学时	拟授课教师	授课学期
算法与数据结构	52	4	王翠青	3
网络空间安全导论	32	2	付强	3
计算机组成原理	52	4	张波	4
数据库系统原理及安全	52	4	韩世迁	4
计算机网络	52	4	王庆辉	3
操作系统及安全	48	3	王旭/吴明旦	5
密码学基础	32	2	李鹏飞	3
Web应用开发	44	2	王璐	4
Web应用安全	44	2	苗春雨	5
网络安全技术	32	1	李莉/孙伟峰	5
渗透测试技术	32	2	郑宇/莫凡	5
软件安全	32	2	关慧	6
大数据技术及安全	40	3	李大舟	5
路由交换原理与技术	32	2	张丽	4
网络攻防技术	32	2	叶雷鹏/杜廷龙	6
工控安全原理	32	2	宗学军	5
工业控制与物联网安全	40	2	王军	6
工业数据安全与合规	32	2	高淑芝	7
无线通信网络安全	32	2	张成	6
网络安全协议分析	48	3	曹克让	6
网络空间安全竞赛实践	36	3	赵今	6
网络空间安全专业实践	72	3	李莉	7

6.2本专业授课教师基本情况表

姓名	性别	出生年月	拟授课程	专业技术职务	学历	最后学历毕业学校	最后学历毕业专业	最后学历毕业学位	研究领域	专职/兼职
王军	男	1978-09	工业控制与物联网	教授	研究生	中国科学院沈阳自	机械电子工程	博士	网络安全	专职

			安全			动化研究所				
李莉	女	1978-09	网络安全技术	教授	研究生	北京邮电大学	机械电子工程	博士	物联网、无线传感器网络	专职
宗学军	男	1970-01	工控安全原理	教授	研究生	东北大学	计算机应用技术	硕士	工业互联网平台安全	专职
王庆辉	男	1972-05	计算机网络	教授	研究生	东北大学	计算机应用	博士	计算机网络与安全	专职
高淑芝	女	1968-04	工业数据安全与合规	教授	研究生	东北大学	控制理论与控制工程	博士	智能优化控制	专职
张波	女	1979-12	计算机组成原理	副教授	研究生	沈阳工业大学	研究生	博士	人工智能与计算机视觉	专职
王旭	男	1983-08	操作系统及安全	副教授	研究生	东北大学	系统工程	博士	应急网络建模与鲁棒优化，智能决策理论与方法，制造与服务系统建模与优化，计算智能	专职
关慧	女	1976-12	软件安全	副教授	研究生	英国德蒙福特大学	软件工程	博士	软件安全	专职
曹克让	男	1981-09	网络安全协议分析	副教授	研究生	韩国培才大学	计算机工学	博士	智能优化算法开发与设计	专职
李大舟	男	1982-06	大数据技术及安全	副教授	研究生	东北大学	研究生	博士	人工智能与大数据	专职
张成	男	1980-08	无线通信网络安全	副教授	研究生	东北大学	研究生	博士	过程安全控制	专职
罗威	女	1967-06	网络空间	副教授	大学本科	辽宁大学	本科	学士	应用数学	专职

			安全数学基础							
韩世迁	男	1973-06	数据库系统原理及安全	副教授	研究生	吉林大学	应用物理学	硕士	人工智能药物研发	专职
王翠青	女	1978-02	算法与数据结构	讲师	研究生	东北大学	计算机系统结构	硕士	编译技术	专职
付强	男	1990-05	网络空间安全导论	讲师	研究生	东北大学	计算机系统结构	博士	网络安全，工业互联网	专职
李鹏飞	男	1988-11	密码学基础	讲师	研究生	东北大学	计算机科学与技术	博士	知识图谱，大语言模型	专职
张丽	女	1979-04	路由交换原理与技术	讲师	研究生	辽宁石油化工大学	计算机技术	硕士	网络通信与安全	专职
王璐	女	1979-09	Web应用开发	讲师	研究生	沈阳化工大学	计算机应用	硕士	软件架构	专职
张静	女	1981-09	数据库系统原理及安全	讲师	研究生	沈阳化工大学	计算机应用	硕士	数据挖掘	专职
阎晨阳	男	1992-04	网络空间安全导论	讲师	研究生	日本国立金泽大学	电子信息科学	博士	类脑计算	专职
赵今	男	1996-07	网络空间安全竞赛实践	其他中级	大学本科	北京联合大学	软件工程	学士	网络信息安全	兼职
郑宇	男	1996-04	渗透测试技术	其他中级	大学本科	西安电子科技大学	信息安全	学士	网络信息安全	兼职
杜廷龙	男	1977-02	网络攻防技术	其他正高级	研究生	北京工业大学	电路与系统	硕士	网络信息安全	兼职
孙伟峰	男	1978-05	网络安全技术	其他正高级	研究生	西安科技大学	通信与信息系统	硕士	网络信息安全	兼职
莫凡	男	1990-06	渗透测试技术	其他正高级	研究生	浙江大学	电子通信工程	硕士	网络信息安全	兼职
叶雷鹏	男	1995-08	网络攻防技术	其他正高级	大学本科	杭州电子科技大学	信息安全	学士	网络信息安全	兼职
苗春雨	男	1979-07	Web 应用	其他正高	研究生	浙江工业	控制科学	博士	网络信息	兼职

			安全	级		大学	与工程		安全	
吴鸣旦	男	1982-03	操作系统及安全	其他正高级	大学本科	浙江大学	计算机科学与技术	学士	网络信息安全	兼职

6.3教师及开课情况汇总表

专任教师总数	20		
具有教授（含其他正高级）职称教师数	11	比例	39.29%
具有副教授及以上（含其他副高级）职称教师数	19	比例	67.86%
具有硕士及以上学位教师数	23	比例	82.14%
具有博士学位教师数	14	比例	50.00%
35岁及以下青年教师数	6	比例	21.43%
36-55岁教师数	20	比例	71.43%
兼职/专职教师比例	8:20		
专业核心课程门数	22		
专业核心课程任课教师数	28		

7.专业主要带头人简介

姓名	王军	性别	男	专业技术职务	教授	行政职务	院长
拟承担课程	工业控制与物联网安全			现在所在单位	沈阳化工大学		
最后学历毕业时间、学校、专业		博士研究生，2009.01中国科学院沈阳自动化研究所，机械电子工程					
主要研究方向		工业互联网，网络安全，物联网					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		项目： 1、教育部就业育人项目“面向产教融合的网络安全人才实践能力培养与实践”教学司函〔2023〕6号 2、教育部产学合作协同育人项目“产教融合视域下网络安全人才实践能力培养”2024年08月批次 获奖： 2022年辽宁省教学成果奖二等奖（排名第一） 2022年辽宁省教学成果奖二等奖（排名第四）； 2022年研究生教学成果奖二等奖（排名第五） 2022年辽宁省教学成果奖三等奖（排名第六） 2018年辽宁省教学成果三等奖（排名第二）； 辽宁省教学名师；					
从事科学研究及获奖情况		项目： 1、工业软件测试平台开发（2024210104001042）横向，108万元； 2、面向QoS的工业物联网感知层核心技术研究（G2022006008L），科技部外专项目，40万元； 3、基于工控蜜网的恶意软件抑制策略优化与研究（2022-MS-291），辽宁省自然科学基金面上项目，5万元； 4、一种基于马氏距离的女巫攻击网络节点异常检测方法（2025210104000288），专利成果转化，10万元。 5、辽宁省科技厅应用基础研究计划：面向工业互联网的入侵检测技术及智能防御策略研究（2025-1746669597594），30万元。 获奖： 辽宁省自然科学成果奖2等奖1项，3等奖3项					
近三年获得	5.0			近三年获得	163.0		

教学研究经费（万元）		科学研究经费（万元）	
近三年给本科生授课课程及学时数	授课计算机网络、物联网技术等 学时：192	近三年指导本科毕业设计（人次）	48

<table>
<tr><td>姓名</td><td>李莉</td><td>性别</td><td>女</td><td>专业技术职务</td><td>教授</td><td>行政职务</td><td>副院长</td></tr>
<tr><td>拟承担课程</td><td colspan="3">网络安全技术</td><td>现在所在单位</td><td colspan="3">沈阳化工大学</td></tr>
<tr><td colspan="2">最后学历毕业时间、学校、专业</td><td colspan="6">2008年7月博士毕业于北京邮电大学机械电子工程专业</td></tr>
<tr><td colspan="2">主要研究方向</td><td colspan="6">物联网、无线传感器网络</td></tr>
<tr><td colspan="2">从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）</td><td colspan="6">项目：
1.辽宁省研究生教育教学改革研究项目，以提升实践能力为驱动的计算机类专业学位研究生培养体系研究与实践，2023.01-2024.12，主持。
2.辽宁省研究生教育教学改革研究项目，面向科教融合的计算机类专业研究生实践创新能力培养与探索，2024.01-2025.12，参与。
沈阳化工大学教育教学改革培育项目，新工科专业中网络编程类课程的多元化-全过程考核方式探索，2025.01-2026.12，主持。
获奖：
2020年12月获沈阳化工大学教学成果二等奖</td></tr>
<tr><td colspan="2">从事科学研究及获奖情况</td><td colspan="6">项目：
1.辽宁省高等学校基本科研项目，基于涡致振动的剪切模式压电俘能结构研究，2023.12-2025.12，主持。
2.辽宁省高等学校基本科研项目，面向无线传感器网络的数据融合隐私保护算法优化研究，2022.12-2024.12，参与。
辽宁省高等学校基本科研项目，无线传感器网络部署优化策略研究
，2022.12-2024.12，主持。
获奖：
2010年12月获国防科学技术进步二等奖
2012年3月获北京市科学技术三等奖
2009年12月中国电子学会电子信息科学技术三等奖</td></tr>
<tr><td>近三年获得教学研究经</td><td colspan="3">3.0</td><td>近三年获得科学研究经</td><td colspan="3">5.0</td></tr>
</table>

费（万元）		费（万元）	
近三年给本科生授课课程及学时数	授课：网络编程技术、网络安全技术等 学时：240	近三年指导本科毕业设计（人次）	45

姓名	宗学军	性别	男	专业技术职务	教授	行政职务	发展规划处处长
拟承担课程	工控安全原理			现在所在单位	沈阳化工大学		
最后学历毕业时间、学校、专业		2003.07 东北大学 计算机应用技术 硕士					
主要研究方向		工业互联网平台安全防护体系建设； 新型工控架构的漏洞挖掘系统研发； 工业网络协议逆向与加密技术研究； 工业网络攻击溯源与系统根因分析。					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		2018年辽宁省普通高等教育教学成果三等奖（研究生类） 第一完成人 2018年沈阳化工大学教学成果奖（研究生类）一等奖 第一完成人 2022年辽宁省首届优秀研究生导师 2022年辽宁省教学成果（研究生类）一等奖 第一完成人 2023辽宁省优秀硕士学位论文指导教师					
从事科学研究及获奖情况		项目： 2023年辽宁省科学技术计划项目-“揭榜挂帅”技术攻关项目 58万 2024年辽宁省科技重大专项（[2024] 4号(3)）200万 2025年AI赋能的金融领域信息安全防御体系架构开发 72万 获奖： 2009年辽宁省科技厅 科技进步二等奖 第一完成人 2009年第三届沈阳市百佳技术创新能手 2011年辽宁省百千万人才工程百人层次 2013年全国石油和化工优秀科技工作者 2015年中国石油和化工工业联合会 科技进步二等奖 第一完成人 2021年辽宁省“兴辽英才计划”科技创新领军人才 2023年享受政府特殊津贴人员					

近三年获得教学研究经费（万元）	0.8	近三年获得科学研究经费（万元）	716.0
近三年给本科生授课课程及学时数	授课：工控安全原理、工业网络协议等 学时：288	近三年指导本科毕业设计（人次）	31

姓名	王庆辉	性别	男	专业技术职务	教授	行政职务	网络与信息化中心主任
拟承担课程	计算机网络			现在所在单位	沈阳化工大学		
最后学历毕业时间、学校、专业		2006年4月，东北大学，计算机应用，工学博士					
主要研究方向		计算机网络与安全					
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）		作为负责人，获得辽宁省研究生教学成果二等奖1项，校研究生教学成果二等奖1项，三等奖1项。作为主要完成人，获辽宁省教学成果二等奖1项。					
从事科学研究及获奖情况		承担企业横向课题1项； 作为主要完成人，获辽宁省科技进步三等奖1项，中国石油化工协会科技进步三等奖1项。					
近三年获得教学研究经费（万元）	1.0			近三年获得科学研究经费（万元）	90.0		
近三年给本科生授课课程及学时数	授课：计算机网络 学时：96			近三年指导本科毕业设计（人次）	26		

姓名	高淑芝	性别	女	专业技术职务	教授	行政职务	装备可靠性研究所副所长
拟承担课程	工业数据安全与合规			现在所在单位	沈阳化工大学		
最后学历毕业时间、学校、专业		2012.01 东北大学控制理论与控制工程专业					
主要研究方向		（1）复杂工业过程建模、智能优化控制技术；					

	（2）机械基础件（滚动轴承）可靠性评估与预测技术。
从事教育教学改革研究及获奖情况（含教改项目、研究论文、慕课、教材等）	无
从事科学研究及获奖情况	项目：1.国家自然科学基金面上项目：“模型驱动的滚动轴承及多生态环境优化的运行可靠度评估与预测”（编号：52275156），70万元；（主持人） 2.“NSFC-企业创新发展基金”国家重点基金项目：“高精度直驱式双回转工作台可靠性稳健优化设计与测试方法”（U23B2098），310万元；（主要参与人） 横向课题：高性能材料聚合过程传动系统关键技术研究，15万元；（主持人） 获奖： 作为第一完成人，获得省部级二等奖2项，三等奖2项，成果转化奖1项。 1.《基于TDI合成的聚氯乙烯成套装备关键技术研究及工业化应用》[编号：2016-F-2-04-R01]项目获辽宁省科学技术发明二等奖； 2.《氯乙烯合成增产技术》[编号：2007JBR0048-2-01]获得中国石油和化学工业协会科技进步二等奖； 3.《高强度低成本零污染聚氯乙烯生产优化技术》[编号:2012JBR0248-3-1]项目获中国石油和化学工业联合会科技进步三等奖； 4.《聚氯乙烯全新工艺优化技术》[编号：2010J-3-73-01]项目获辽宁省科技进步三等奖； 5.《氯乙烯合成增产技术》[编号：2007ZH-3-22G01]获辽宁省科技成果转化三等奖

近三年获得教学研究经费（万元）	0.4	近三年获得科学研究经费（万元）	188.0
近三年给本科生授课课程及学时数	授课：可靠性工程 学时：64	近三年指导本科毕业设计（人次）	3

8.教学条件情况表

可用于该专业的教学实验设备总价值（万元）	997.2	可用于该专业的教学实验设备数量（千元以上）	643（台/件）
开办经费及来源	辽宁省政府拨款、沈阳化工大学及计算机科学与技术学院办学经费等		
生均年教学日常运行支出（元）	2980.0		
实践教学基地（个）	23		
教学条件建设规划及保障措施	重点建设工业信息安全实训基地，构建网络安全规划、漏洞评估、防御及灾情分析实训环境，打造护网综合实战靶场，融入传统网络与工业虚拟场景；完善实训资源体系，涵盖产业级实践项目、靶标库等。同时，培育双师型师资，柔性引进企业高级工程师参与授课与指导，安排专任教师到企业实践，组建校企双导师团队。开发数字化教学资源，建设一流课程及教材、案例库，推动“安全技术+行业场景”课程体系落地。 建立政校企协同育人机制，多方参与培养目标、课程设置等环节，形成长效投入与合作机制。定期联合修订培养方案，确保与产业技术迭代同步。依托实训设施开展社会化服务，包括网络安全技能培训、认证及竞赛服务，提升资源利用效率与师资实战能力，为专业持续发展提供支撑。		

主要教学实验设备情况表

教学实验设备名称	型号规格	数量	购入时间	设备价值（千元）
柜式空调	空气精密管理系统 EM17U1	1	2025	38181.0
24口交换机	H3C US1750-28P	1	2025	1600.0
48口交换机	H3C US1750-52P	5	2025	13500.0
路由器	H3C MSR2600-12X-WiNet	1	2025	4700.0
现场模拟环境	无	1	2024	25000.0
工业PC控制柜	无	1	2024	5000.0
无线智能网关	ZAGW1000	1	2024	20000.0
无线智能控制器	ZACL100	1	2024	8500.0
无线压力变送器	ZAPT1120	3	2024	10500.0
无线温度变送器	ZATT1120	3	2024	9000.0
交换机	S1224R	2	2024	2760.0

壁挂式空调	1.5p KFR-35GW/(35523)FNhAa-B3	1	2024	3200.0
柜式空调	3p KFR-72LW/(72565)FNhAc-B3(WIFI)	1	2024	8300.0
微型电子计算机	华为擎云W515 B730-K7851B 显示器B3-241H	30	2024	215700.0
微型电子计算机	华为擎云W515 PGUV-WBY0	10	2024	69900.0
智能协作大屏	IdeaHub Board 2-86寸	2	2024	31960.0
网络平台用服务器	PR210K	2	2024	156000.0
SDN服务器	PR2710P	1	2024	80000.0
视频解析X86服务器	Atlas 800（Model 3010）	1	2024	102000.0
深度学习X86服务器	Atlas 800（Model 3010）	1	2024	255000.0
训练服务器	Atlas 800（Model 9000）	1	2024	575160.0
深度学习服务器	TaiShan 200（Model 2280）	1	2024	105000.0
智能协作大屏支架	HUAWEI Ideahub 白色落地支架	1	2024	2500.0
抗DDOS防火墙	AntiDDoS1905-AC	1	2024	96700.0
防火墙	USG6525E-AC	3	2024	97200.0
AC控制器	AirEngine9700-M1	2	2024	107400.0
无线路由器AP2	AirEngine5761-11	2	2024	3920.0
无线路由器AP1	AirEngine5760-51	2	2024	7800.0
交换机	S5731-H24T4XC	5	2024	61500.0
路由器	AR6121E	5	2024	31500.0
微型电子计算机	H3C uniserverR4900 G3	1	2023	69900.0

微型电子计算机	H3C X5-020t	71	2023	400085.0
投影仪	NEC NP-CR3100H	1	2022	6998.0
微型电子计算机	H3C C207V	1	2021	5845.0
视频摄像头	DS-U102D	2	2021	3980.0
微型电子计算机	HP480	1	2021	7995.0
接入交换机	H3C-5130-S-52P-EI	1	2021	5950.0
微型电子计算机	H3C C207V	37	2021	216265.0
激光打印机	LBP6230DN	1	2019	1599.0
柜式空调	KFR-72LW	1	2019	5900.0
柜式空调	KFR-50LW	10	2019	49500.0
投影仪	E310	1	2019	5500.0
高级智能创新套件	MKMC602G	15	2019	74940.0
计算机组成原理实验系统	COP8000	40	2019	154000.0
瘦终端系统	定制	70	2019	250600.0
投影仪	NEC CR2170X	1	2019	5350.0
接入交换机	E55C	3	2019	21000.0
汇聚交换机	S5560X-30CEI	1	2019	7000.0
微型电子计算机	280 G4 MT	1	2019	5400.0
多媒体讲台	定制	1	2019	2080.0
管理服务器	UIS—Cell 3010 G3	1	2019	60000.0
云桌面超融合服务器	UIS—Cell 3010 G3	2	2019	120000.0
数字图像采集方案套件箱	MV-MVKB	10	2019	58500.0
机器视觉系统应用实验开发平台	MV-VS1200S	10	2019	49800.0
机器视觉算法研究实验平台	MV-VS1000	16	2019	159040.0
智能小车开发平台2（机器人）	ZYRP60B	2	2019	4400.0
智能小车开发平台1（机器人）	ZYRP60BROS	5	2019	12400.0
微型电子计算机	定制	1	2019	3900.0
多媒体讲台	定制	1	2019	5100.0

轻型机柜	图腾42U服务器机柜	1	2019	4000.0
接入交换机	E552C	2	2019	14670.0
汇聚交换机	S5560X-30C-EI	1	2019	6070.0
云桌面超融合服务器	UIS-Cell3010 G3	2	2019	119900.0
虚拟管理平台	H3C虚拟管理平台软件1套	1	2018	129300.0
服务器	H3C UIS R390X	2	2017	126000.0
接入交换机	H3C E552C	2	2017	10500.0
H3C SUN100云终端	H3C	70	2017	94500.0

9. 申请增设专业的理由和基础

申请增设专业的理由和基础

一、申请增设网络空间安全专业的理由

1、 国家战略需求

在数字化时代，网络空间已成为继陆、海、空、天之后的第五大主权领域空间。网络空间安全直接关系到国家的政治安全、经济安全、军事安全和文化安全。近年来，网络攻击事件频发，涉及国家关键信息基础设施、重要数据和个人隐私等领域，给国家安全带来了严重威胁。我国相继出台《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规，明确提出对关键信息基础设施的保护要求，并建立网络安全审查制度。增设网络空间安全专业，培养专业的网络空间安全人才，是维护国家网络空间主权和安全的重要举措，有助于构建国家网络空间安全防御体系，提升国家在网络空间的战略威慑力和应对能力。

2、 产业发展需求

随着互联网、大数据、人工智能、物联网等新兴技术的广泛应用，网络空间安全行业迎来了前所未有的发展机遇。据市场研究机构预测，未来几年全球网络空间安全市场规模将持续增长，我国网络空间安全市场规模也将保持较高的增长率。行业的快速发展对网络空间安全专业人才的需求急剧增加，目前市场上专业人才供给远远不能满足行业需求。根据教育部和艾媒咨询数据，截至 2024 年，我国网络空间安全行业人才缺口已进入加速扩大阶段。国家网信办数据显示，2025 年行业人才缺口已达 200 万人，较 2023 年增长 33%，预计到 2027 年，总缺口将达到 327 万，而相关本科毕业生年规模仅为 1.45 万人，供需比例严重失衡。这一缺口主要驱动由因素为市场规模扩张以及国家政策支持。2023 年中国网络安全市场规模为 683.6 亿元，预计 2027 年增至 884.4 亿元，年复合增长率达 6.7%；国家发改委将网络安全行业列为“鼓励类”，《产业结构调整指导目录（2024 年本）》进一步强化了产业政策导向。增设网络空间安全专业，能够为行业输送大量专业人才，缓解行业人才短缺的压力。

网络攻击手段不断翻新，恶意软件、黑客攻击、数据泄露、网络诈骗等安全威胁日益复杂多样。同时，随着云计算、区块链等新技术的应用，新的安全风险也不断涌现。网络空间安全行业需要具备深厚专业知识和丰富实践经验的专业人才，能够及时发现和应对各种安全威胁，保障网络空间的安全稳定运行。增设网络空间安全专业，通过系统的专业教育和实践训练，培养能够应对复杂安全威胁的专业人才，满足行业对高素质安全人才的需求。

在数字化时代，企业纷纷加快数字化转型步伐，将业务和数据迁移到网络空间。然而，数字化转型也带来了新的安全挑战，企业需要专业的网络空间安全人才来保障其信息系统的安全性和可靠性。增设网络空间安全专业，能够为企业培养适应数字化转型需求的安全专业人才，帮助企业建立健全网络安全管理体系，提高企业的网络安全防护能力。

3、 区域社会发展需求

根据前瞻产业研究院《2024-2029年辽宁省信息安全市场前瞻与投资战略规划分析报告》，辽宁省信息安全市场规模持续扩大，2024年依托数据安全法规强制实施市场规模为68-72亿元，到2026年收到工业互联网安全平台建成驱动市场规模预计能达到90-98亿元，2029年市场规模更是能达到130-145亿元。2023年网络安全人才缺口已达11万人(需求59万人，实际供给48万人)。随着数字辽宁、智造强省战略推进，预计到2027年缺口将进一步扩大，特别是工业互联网、关键信息基础设施防护等领域需求迫切。

辽宁省内只有辽宁大学、沈阳工程学院、辽宁警察学院、大连东软信息学院四所高校设置网络空间安全专业，但年均培养量不足400人，远低于工业互联网、政务数字化等领域激增的需求，不足以支撑区域经济发展需求。

4、 专业群建设需求

我校一直致力于学科专业的优化和升级，以适应社会发展的需求。增设网络空间安全专业，能够进一步完善我校的学科专业体系，填补我校在网络空间安全领域的专业空白，提升我校在信息技术领域的学科竞争力。同时，该专业的建设也将促进我校与其他相关学科的交叉融合，推动学科创新和发展。

网络空间安全专业是一个综合性、实践性很强的专业，涉及计算机科学、数学、通信工程、法学等多个学科领域。增设该专业，我校将整合校内外优质教育资源，构建完善的课程体系和实践教学平台，加强师资队伍建设，提高教学质量和人才培养水平。通过该专业的培养，学生将具备扎实的专业基础知识、较强的实践能力和创新精神，能够适应网络空间安全行业的发展需求。

我校作为地方高校，始终以服务地方经济社会发展为己任。增设网络空间安全专业，能够为地方网络安全产业的发展提供人才支持和技术服务。通过与地方企业、政府部门的合作，开展产学研项目，推动网络安全技术的研发和应用，促进地方网络安全产业的升级和发展，为地方经济社会发展做出积极贡献。

增设网络空间安全专业是响应国家战略、填补行业人才缺口、优化学科布局的必然选择。通过整合政策支持、产业资源与学术积累，培养兼具理论素养和实战能力的高端人才，可为网络强国建设提供核心支撑，助力我国在全球网络空间竞争中占据主动地位。

二、专业建设基础

沈阳化工大学是以工为主，以化工为特色，工学、理学、管理学、经济学、文学、法学、医学等7大学科门类相结合的多科性综合大学。计算机学院现有计算机科学与技术、软件工程、网络工程、数据科学与大数据技术4个本科专业。其中计算机科学与技术专业为国家一流建设专业、辽宁省一流建设专业、辽宁省工程人才培养模式改革试点专业、辽宁省普通本科高等学校向应用型转变示范专业并通过了国家工程教育认证。软件工程、网络工程为辽宁省一流建设专业。计算机科学与技术一级学科拥有理学和工学学术硕士学位授予权以及电子

信息专业硕士学位授予权，具有计算机应用技术和计算机软件与理论两个二级学科。专业硕士学位涉及计算机技术、大数据技术与工程以及网络与信息安全专业领域。学院于 2024 年入选工业与信息化部工业信息安全人才培养专项行动计划高等院校实施单位。学科基础可以为本专业建设提供必要的支持。

计算机科学与技术学院设有电子信息专业硕士计算机网络与安全方向，主要涉及物联网与网络空间安全技术的研究与产品研发，包括物联网感知层相关技术研究；“互联网+”相关应用技术研究；工业物联网及智能制造相关技术的演示与验证平台研发；基于“互联网+工业”的网络安全技术研究；水下物联网相关技术研究等。特别围绕我省化工过程工业产业智能化升级需求，以解决化工过程工业信息化、智能化为目标进行相关技术研究。学院现有辽宁省化工过程工业智能化技术重点实验室、工业物联网技术国家与地方共建实验实践基地、计算机科学与技术辽宁省实验教学示范中心以及沈阳市化工工业数智化技术重点实验室等省市级以上教学和科研平台 4 个。基于以上创新平台，学校已经申请工业网络安全数项相关领域的科研项目，培养研究生 20 余名，拥有人才培养的良好平台基础。

拟增设的网络空间安全专业拥有专职教师 20 人，其中教授 5 人，副教授 8 人，讲师 7 人，具有博士以上学历 13 人。此外，在网络空间安全企业聘任外聘实践教学类教师 8 人。师资队伍在年龄、学历和学科领域结构合理，具有核心骨干课程的授课条件。

学院实验室面积 1100 多平方米，拥有工业互联网仿真平台、水下传感器网络仿真和测试平台、华为 ICT 实验室、网络攻防实训平台、大数据实训平台、深度学习服务器、视频解析服务器等实验设备和平台，可以满足新专业建设的实验实践需求。

学校注重产学研合作，目前在计算机学科领域与企业建立广泛的联系，通过“产学研”结合的办学模式，获得企业对学校教学的支持，为学生实习提供稳定的实习基地，实现校企合作，为学生提供参与工程实践的平台，从而保证教学目标实现的有效途径。目前拥有正式签订合作协议的教学实践基地 23 个。目前，沈阳化工大学计算机科学与技术学院可提供专业学生实习实训工作的基地有 15 家单位。通过校内外实习和实训基地深化实践教学内涵，改革实践教学模式，健全保障体系，建立了校企合作长效机制，可以为网络空间安全专业的人才培养提供必要的支持。

三、专业发展规划

1、专业建设目标

网络空间安全专业立足国家网络安全战略，聚焦东北老工业基地数字化转型需求，坚持立德树人根本任务，秉持“育人为本，服务产业，产教融合，创新发展”的理念，以培养产业高素质人才、提升教学能力、服务当地社会、促进产业发展为目标。围绕网络安全战略新兴产业和传统产业升级，构建紧密对接产业链、创新链的人才培养体系；围绕行业生产需求设计课程体系和教学环节，强化产教融合实训环境、平台和载体建设，革新学生创新实践能力培养机制，提升教师数字化专业育人能力。充分发挥高校与地方政府、企业机构等双方或

多方协同育人模式，整合多主体创新要素和资源，通过建设网络空间安全专业推进“政校企”可持续、内涵式创新发展。

（1）深化政校企产教融合

形成多元主体协同育人的实践培养机制。建立政校企行多方投入协同育人机制体制，深度参与学生培养工作，从培养目标、课程设置、教材编制、实验室建设、实践教学等各个环节组织机制，推动政校企协同育人。

（2）建设数字化教学实践平台

构建“从生产中来，到生产中去”的特色育人模式。通过引入典型网络安全生产实践项目、企业真实网络安全课题，从实际网络安全生产应用所需的知识、技术和技能出发，将网络安全新方法、新技术、新工艺、新标准引入教育教学实践，形成“在网络安全生产中学习，在学习中进行网络安全生产”的培养模式，构建真实网络安全职业环境下的实践育人模式。

（3）打造校企“互聘共用、双向交流”的双师结构教学团队

组建网络安全产教融合实践项目校企双导师团队，双方师资相互融合、互为补充、形成合力；构建双导师队伍培养机制，企业导师参与网络空间安全专业课程教学任务，指导网络安全实践教学，与学校专任教师共同开展网络安全教学研究，学校教师到企业进行网络安全岗位实践、参与企业网络安全工程实践，提升专业群教师的教学、科研和网络安全技术服务能力。

（4）立足辽宁，面向政企单位开展网络安全技能培训及竞赛服务

依托网络空间安全专业实训设施及教学资源，政府导入东北区域能源、运营商、金融、公安等行业人才培养需求，如 CISP 等职业认证培训考试、网络安全红蓝队技能培训、攻防演练实训等，面向政企单位开展数字安全技能培训、技能竞赛，为人才培养、人才选拔提供数字服务。

2、专业建设任务

（1）建设高水平数字化专业

专业建设主动对接数字安全产业，围绕国家和省内网络安全数字经济产业布局，调整专业结构，凝练办学特色，打造优势专业；依据数字安全产业发展前沿趋势，建设产业急需专业，培养行业紧缺的网络空间安全人才。

①优化人才培养方案

以国家相关政策、专业设置规范及产业人才标准为指导，基于 OBE（成果导向教育）理念，明确网络空间安全专业人才培养目标与毕业要求的对应关系，通过反向设计课程体系，确保教学内容与产业需求深度契合。导入合作企业凝练产业最佳实践形成的标准课程、真实案例、业务场景、实战项目等教学资源，政府、企业深度参与专业人才培养方案建设过程，共同研究专业人才培养内容，遵循 CDIO 工程教育模式（构思-设计-实现-运作），将网络空

间安全工程实践贯穿于课程设置全流程，重点融入工业互联网安全架构设计、网络安全攻防工程实施等真实工程场景。

跨学科对知识进行整合，有机融合网络空间安全知识、法律法规、工业网络安全、工程伦理与综合能力培养，建立“知识-技能-伦理”三位一体的课程体系。在实践能力培养方面，通过“项目式学习”“案例教学”等方式，将企业实战项目转化为教学模块，实现“做中学、学中做”的工学结合模式。构建专业持续改进机制，建立毕业要求达成度评价体系，定期联合政校企三方开展培养方案修订，确保人才培养质量与产业技术迭代同步。

以多方协同、工学结合的人才培养模式，提升专业学生的工程基础素养、网络安全专业知识、跨学科学习能力，实现“解决复杂网络安全工程问题”的应用型人才培养目标，同时强化学生的工程伦理意识与社会责任，使其具备网络安全领域的工程实践创新能力。

②提升专业建设质量

网络空间安全专业成立专业建设委员会，从专业基础、专业配套、专业扩展三个层面，实现高水平专业建设。提升专业建设质量包括课程体系、师资队伍、教材教辅、实习实训、人才就业、技能比赛、人才评价、职业素养、就业推荐等方面，积累数字安全高技能人才培养经验，为高水平专业群建设提供有力基础。

在专业群设计方面，立足工业应用场景，实现多专业交叉复合，参考真实网络安全岗位知识技能要求，校企共同研究网络空间安全专业人才培养内容，共同确定人才培养规格、课程体系、教学内容、教学方式和学生学业考核评价方法，为培养工业互联网安全人才奠定基础。

③开发数字化教学资源

根据相关网络空间安全课程知识图谱，优化、补充教学资源，将工业互联网安全、工业信息安全知识、技能进行有机融合，促进网络安全产业岗位需求的知识体系及交叉技术应用体系的完善；按照教育部“一流课程”建设指导思想，依据线上、线下、混合式、虚拟仿真和社会实践五大“一流课程”建设标准，开展一流网络空间安全课程建设；同时开展网络空间安全教材、实验指导书、网络安全项目案例等教学资源建设。

（2）实习实训基地建设

在现有资源的基础上优化升级，结合区域经济、产业升级需求，围绕网络安全产业技术应用、网络安全科研创新场景，建设场景化、浸润式的工业信息安全人才培养基地，开发相关网络安全工程训练项目资源，支撑相关学科与专业开展项目式、启发式、创新式教学改革，及网络安全科研创新与社会服务。

①工业信息安全实训基地建设

构建网络安全规划、安全漏洞评估、网络防御和安全灾情分析等实训环境，加大对学生网络安全规划、渗透测试、应急响应及溯源取证四项核心基础能力的培养；构建网络安全护

网综合实战靶场，靶场融入传统网络、工业领域等相关虚拟场景，培养学生在不同场景下的网络安全综合能力应用，为适应网络安全产业发展需求打下良好基础。

②工业信息安全人才培养实训基地资源建设

完善实训资源体系，构建特色网络安全实训教学资源，涵盖传统网络安全、数据安全、系统安全、工控安全等众多领域，包括产业级网络安全实践项目、项目指导书、实训实验手册、试题等，同时，完善靶标库、工具库、漏洞库等网络安全实训资源，为网络安全实训教学提供资源保障基础。

（3）培育双师型师资

根据工作的需要以柔性人才引进方式，聘请合作企业的高级网络安全工程师、网络安全专家以"企业导师"或"客座讲授"的方式参与网络空间安全专业授课、专业报告、毕业研究课题的技术指导等。同时，学院每年可指派专任教师到企业进行网络安全实践锻炼，企业委派网络安全专家对专任教师进行针对性教学辅导培训，为网络空间安全专业师资的教学质量提供充足的质量把关工作。

①双师结构教学

合作企业安排企业导师进行网络安全专业核心课授课，参与网络空间安全人才培养过程。校企双导师共同授课和指导学生网络安全实践，由学校教师完成通识课、专业基础课教学，企业导师参与网络安全专业核心课、特色方向课部分。学生可参与专属网络安全实践项目、网络安全职业技能竞赛，学生毕业实习推荐进入合作企业以及相关网络安全产业链单位，并在实习的基础上，由双方教师共同指导完成相关网络安全毕业设计。

②师资研修

学校指派专任教师参加合作企业开展的寒暑期师资研修班，内容围绕网络空间安全专业建设主题，采取专家主题报告、分类辅导和互动交流相结合的形式，介绍网络空间安全学科发展前沿、学科建设现状及招生需求，讲解网络安全领域的基础研究、应用研究、关键技术，参观知名互联网和网络安全企业，深度了解网络安全产业人才需。

（4）提升社会服务

通过建设网络空间安全专业，提供社会化服务，包括网络安全能力提升培训、网络安全认证培训业务，承接市级、省级网络安全技能竞赛服务等，为区域网络安全保卫工作提供助力，为区域网络安全人才培养和地方发展贡献力量。

①网络安全培训服务

专业面向社会企事业单位开展网络安全培训服务，从网络安全意识培训到技能培训，从技术层面的 CTF 竞赛培训，再到内外网渗透、应急响应等高阶技能知识，以及 CISP 等安全认证培训，形成完整的网络安全课程服务资源。帮助企事业单位加速网络安全人才体系建设，落地政策相关要求。

②网络安全竞赛服务

网络空间安全专业打造具备网络安全职业技能大赛策划组织能力，可支持竞赛活动的“准备阶段”、“实施阶段”、“成果阶段”、“总结阶段”，支撑各类主流网络安全竞赛模式，如理论知识考核、CTF 夺旗赛、AWD 攻防对抗赛、靶场综合渗透赛、数据安全分析赛、应急响应赛等。

3.预期效果

专业聚焦重点任务建设，充分发挥产教深度融合，推动政校企联合培养，带动我校数字安全专业群建设取得以下预期成果:

(1) 专业建设方面

优化人才培养方案，课程内容与职业标准对接，符合区域产业发展用人需求；学校老师承担专业基础课教学；企业导师承担的专业核心课授课不少于 4 门/届；开展竞赛培训，学生参加各级网络安全技能大赛比例高，省级及以上竞赛成绩优异；建设数字化课程 4 门，编写专业教材 4 本；面向本校学生开展网络与信息安全管理员职业技能等级认定、CISAW 预备级认证等。

预期成果：（1）申报省市级教学成果奖；（2）指导学生参加省级、国家级竞赛，力争获得省级二等奖及以上成绩

(2) 实验室建设方面

建设网络安全数字化实验室 2 个，预期成果：（1）成立校内、校外实训基地；（2）具备举办网络安全技能大赛的承办、选拔、培训的平台和能力

(3) 师资培训方面

每年至少选派 4 名教师参加暑期师资研修班培训，预期成果：（1）学校建培育“双师型”教师不少于 4 名，至少 2 名教师具备专业核心课的授课能力；（2）教师在学科建设竞赛中取得省级及以上教学成果奖

(4) 社会服务方面

合作开展技能培训、职业认证、竞赛演练等社会服务，预期成果：（1）面向在校生、社会从业人员开展 CISP 系列、CISAW 系列、CCRC 系列、人社部网络与信息安全管理员等认证培训；（2）承办区域网络安全竞赛及攻防演练

10. 校内专业设置评议专家组意见表

校内专业设置评议专家组意见表

<table>
<tr><td colspan="2">总体判断拟开设专业是否可行</td><td>☑是　　□否</td></tr>
<tr><td colspan="3">理由：
　　该专业的申报具有充分的区域发展需求依据和扎实的办学基础，有利于适应社会网络空间安全人才培养需求，符合学校整体专业发展规划，培养方案具体，课程设置合理，师资队伍力量雄厚，实践条件比较优越，经费保障充足，预测学生有较好的就业前景。学校现有专业建设基础、师资力量及结构、实践教学条件能较好地支撑该专业的开设。
　　提出的建议：网络空间安全研究发展迅速，建议紧跟研究前沿，增设特色内容；进一步加大专业建设投入，优化实验资源配置。
　　同意推荐增设网络空间安全本科专业。</td></tr>
<tr><td colspan="2">拟招生人数与人才需求预测是否匹配</td><td>☑是　　□否</td></tr>
<tr><td rowspan="3">本专业开设的基本条件是否符合教学质量国家标准</td><td>教师队伍</td><td>☑是　　□否</td></tr>
<tr><td>实践条件</td><td>☑是　　□否</td></tr>
<tr><td>经费保障</td><td>☑是　　□否</td></tr>
<tr><td colspan="3">专家签字：</td></tr>
</table>